

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-131923

(P2003-131923A)

(43) 公開日 平成15年5月9日 (2003.5.9)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
G 0 6 F 12/00	5 3 7	G 0 6 F 12/00	5 3 7 Z 5 B 0 6 5
	5 1 4		5 1 4 E 5 B 0 8 2
	5 4 5		5 4 5 A 5 K 0 3 0
3/06	3 0 4	3/06	3 0 4 H
H 0 4 L 12/56		H 0 4 L 12/56	H

審査請求 未請求 請求項の数34 O L 外国語出願 (全 48 頁)

(21) 出願番号 特願2002-114116(P2002-114116)
 (22) 出願日 平成14年4月17日 (2002.4.17)
 (31) 優先権主張番号 09/839952
 (32) 優先日 平成13年4月19日 (2001.4.19)
 (33) 優先権主張国 米国 (US)

(71) 出願人 000005108
 株式会社日立製作所
 東京都千代田区神田駿河台四丁目6番地
 (72) 発明者 岩見 直子
 アメリカ合衆国カリフォルニア州クバティ
 ーノ アパートメント #6211 プルネリッ
 ジアベニュー 19500
 (74) 代理人 100075096
 弁理士 作田 康夫
 Fターム(参考) 5B065 BA01 CH04 PA01 PA12
 5B082 EA11 FA07 HA00
 5K030 GA08 GA15 HA08 HCO1 HD03
 HD07 KA07

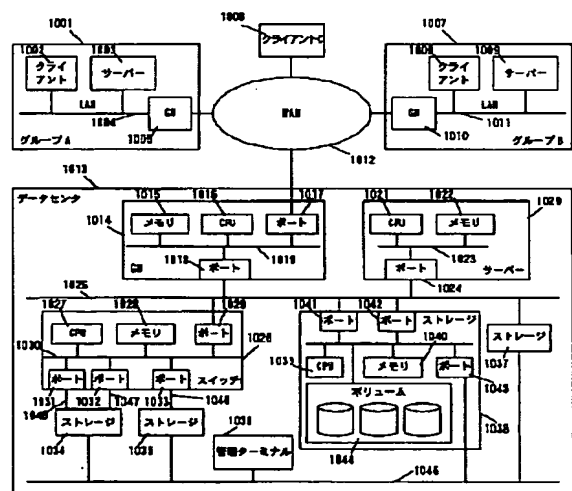
(54) 【発明の名称】 仮想プライベートボリューム方式及びシステム

(57) 【要約】

【課題】本発明は、ストレージ資源へのアクセスを管理する技術を提供する。

【解決手段】本発明の実施により、ユーザは、仮想アドレスと仮想ボリューム識別子のシステムを用いて、ストレージデバイス内の資源にアクセスできる様になる。本発明の実施により、企業体を含めてユーザが、インターネットまたは他の種類のネットワークを経由して、ユーザのネットワークでSSP (Storage Service Provider) 内のボリュームを使用することが可能になる。本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシーを確立することができる。

【図1】



【特許請求の範囲】

【請求項1】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも1つのポートを持つゲートウェイと、
それぞれが複数のボリュームの少なくとも1つで構成され、情報を記憶する複数のデバイスの少なくとも1台とサーバーと、
スイッチと、
前記ゲートウェイ、前記サーバー、前記スイッチ、及び情報を記憶する前記複数のデバイスの少なくとも1台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記ゲートウェイは、保存のためにデータパケットを受信し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、該仮想受信アドレスに対応して情報を記憶する前記複数のデバイスの少なくとも1台の特定の1台を指定する受信アドレスを前記メモリから読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。

【請求項2】請求項1記載のストレージ装置において、前記ゲートウェイは、前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。

【請求項3】請求項1記載のストレージ装置において、前記外部ネットワークは、VPN (Virtual Private Network) で構成され、前記ゲートウェイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。

【請求項4】請求項1記載のストレージ装置において、前記外部ネットワークは第1のプロトコルを使用し、前記内部ネットワークは第2のプロトコルを使用し、前記ゲートウェイは前記データパケットを前記第1のプロトコルから前記第2のプロトコルに変換することを特徴とするストレージ装置。

【請求項5】請求項4記載のストレージ装置において、前記第1のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項6】請求項4記載のストレージ装置において、前記第2のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項7】請求項7記載のストレージ装置において、前記ゲートウェイは前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想受信アドレスを、前記検出されたボリューム識別子で置き換えることを特徴とするストレージ装置。

ーム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。

【請求項8】請求項1記載のストレージ装置において、前記ゲートウェイは前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。

【請求項9】請求項1記載のストレージ装置において、前記仮想受信アドレスと前記受信アドレスはテーブルに格納されていることを特徴とするストレージ装置。

【請求項10】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも1つのポートより構成されるサーバーと、
情報を記憶し、各々は少なくとも1つのボリュームで構成される少なくとも1台のデバイスと、スイッチと、前記サーバー、前記スイッチ、および情報を記憶する前記複数のデバイスの少なくとも1台を接続する内部ネットワークと、で構成されるストレージ装置において、
前記サーバーはデータパケットを受信してこれを保存し、前記メモリを検索して前記データパケットから読み出した仮想受信アドレスを検出し、前記メモリより前記仮想受信アドレスに対応して前記デバイスの特定の1台を指定する受信アドレスを読み出し、前記データパケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。

【請求項11】請求項10記載のストレージ装置は、さらに、ゲートウェイから構成され、前記ゲートウェイは、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも1つのポートを有し、前記外部ネットワークは第1のプロトコルを使用し、前記内部ネットワークは第2のプロトコルを使用し、前記ゲートウェイは前記データパケットを前記第1のプロトコルから前記第2のプロトコルに変換することを特徴とするストレージ装置。

【請求項12】請求項11記載のストレージ装置において、前記第1のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項13】請求項11記載のストレージ装置において、前記第2のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項14】請求項11記載のストレージ装置において、前記外部ネットワークはVPN (Virtual Private Network) で構成され、前記ゲートウェイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。

レージ装置。

【請求項 1 5】請求項 1 0 記載のストレージ装置において、前記サーバーは前記データバケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データバケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。

【請求項 1 6】請求項 1 0 記載のストレージ装置において、前記サーバーは前記外部ネットワークに送信されるデータバケットを受け取り、前記メモリを検索して前記データバケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データバケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。

【請求項 1 7】請求項 1 0 記載のストレージ装置において、前記サーバーは前記データバケット内のユーザアドレスに基づいて前記データバケットの送信者を認証することを特徴とするストレージ装置。

【請求項 1 8】プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも 1 つのポートより構成されるスイッチと、情報を記憶し各々は複数のボリュームの少なくとも 1 つで構成される複数のデバイスの少なくとも 1 台と、サーバーと、前記サーバー、前記スイッチ、および情報を記憶する前記複数のデバイスの少なくとも 1 台を接続する内部ネットワークと、で構成されるストレージ装置において、前記スイッチはデータバケットを受信してこれを保存し、前記メモリを検索して前記データバケットから読み出した仮想受信アドレスを検出し、前記メモリから前記仮想受信アドレスに対応して情報を記憶する前記複数のデバイスの少なくとも 1 台の特定の 1 台を指定する受信アドレスを読み出し、前記データバケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。

【請求項 1 9】請求項 1 8 記載のストレージ装置は、さらに、ゲートウェイから構成され、前記ゲートウェイは、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも 1 つのポートを有し、前記外部ネットワークは第 1 のプロトコルを使用し、前記内部ネットワークは第 2 のプロトコルを使用し、前記ゲートウェイは前記データバケットを前記第 1 のプロトコルから前記第 2 のプロトコルに変換することを特徴とするストレージ装置。

【請求項 2 0】請求項 1 9 記載のストレージ装置において、前記第 1 のプロトコルは、IP プロトコル、ATM、及

微とするストレージ装置。

【請求項 2 1】請求項 1 9 記載のストレージ装置において、前記第 2 のプロトコルは、IP プロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項 2 2】請求項 1 9 記載のストレージ装置において、前記外部ネットワークは VPN (Virtual Private Network) で構成され、前記ゲートウェイは前記データバケットに対して VPN 処理を実行することを特徴とするストレージ装置。

【請求項 2 3】請求項 1 8 記載のストレージ装置において、前記スイッチは前記データバケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データバケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。

【請求項 2 4】請求項 1 8 記載のストレージ装置において、前記スイッチは前記外部ネットワークに送信されるデータバケットを受け取り、前記メモリを検索して前記データバケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データバケットの前記受信アドレスを前記メモリから読み取った前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。

【請求項 2 5】請求項 1 8 記載のストレージ装置において、前記スイッチは前記データバケット内のユーザアドレスに基づいて前記データバケットの送信者を認証することを特徴とするストレージ装置。

【請求項 2 6】情報を記憶し、各々は複数ボリュームの少なくとも 1 つ、プロセッサ、メモリ、及び外部ネットワークに接続するための少なくとも 1 つのポートから構成される複数のデバイスの少なくとも 1 台と、スイッチと、サーバーと、前記サーバー、前記スイッチ、および前記情報を記憶する複数デバイスの少なくとも 1 台を接続する内部ネットワークと、で構成されるストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも 1 台はデータバケットを受信してこれを保存し、前記メモリを検索して前記データバケットから読み出した仮想受信アドレスを検出し、前記メモリから前記仮想受信アドレスに対応して前記情報を記憶する複数のデバイスの少なくとも 1 台の特定の 1 台を指定する受信アドレスを読み出し、前記データバケットの前記仮想受信アドレスを前記メモリから読み出した前記対応する受信アドレスに置き換えることを特徴とするストレージ装置。

【請求項 2 7】請求項 2 6 記載のストレージ装置は、さらに、ゲートウェイから構成され、前記ゲートウェイは、プロセッサ、メモリ、及び外部ネットワークに接続

するための少なくとも1つのポートを有し、前記外部ネットワークは第1のプロトコルを使用し、前記内部ネットワークは第2のプロトコルを使用し、前記ゲートウェイは前記データパケットを前記第1のプロトコルから前記第2のプロトコルに変換することを特徴とするストレージ装置。

【請求項28】請求項27記載のストレージ装置において、前記第1のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項29】請求項27記載のストレージ装置において、前記第2のプロトコルは、IPプロトコル、ATM、及びファイバチャネルの少なくとも一つから成ることを特徴とするストレージ装置。

【請求項30】請求項27記載のストレージ装置において、前記外部ネットワークはVPN (Virtual Private Network)で構成され、前記ゲートウェイは前記データパケットに対してVPN処理を実行することを特徴とするストレージ装置。

【請求項31】請求項26記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも1台は、前記データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出できたら、前記メモリを検索して前記仮想プライベートボリューム識別子に対応するボリューム識別子を検出し、前記データパケットの前記仮想プライベートボリューム識別子を前記ボリューム識別子で置き換えることを特徴とするストレージ装置。

【請求項32】請求項26記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも1台は、前記外部ネットワークに送信されるデータパケットを受け取り、前記メモリを検索して前記データパケットから読み出した受信アドレスを検出し、前記メモリから対応する仮想受信アドレスを読み取り、前記データパケットの前記受信アドレスを前記メモリから読み出した前記対応する仮想受信アドレスで置き換えることを特徴とするストレージ装置。

【請求項33】請求項26記載のストレージ装置において、前記情報を記憶する複数のデバイスの少なくとも1台は、前記データパケット内のユーザアドレスに基づいて前記データパケットの送信者を認証することを特徴とするストレージ装置。

【請求項34】ストレージを管理する方法であって、前記方法は、
データパケットを受信し、
前記データパケットから抽出した仮想受信アドレスを検索し、
前記仮想受信アドレスに対応し、情報を記憶する複数のデバイスの少なくとも1台の特定の1台を指定する受信

前記データパケットの前記仮想受信アドレスを前記対応する受信アドレスで置き換えることから構成されることを特徴とする方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、一般的にデータストレージシステムに関連し、特に、仮想ボリュームを用いてストレージアクセスを制御する技術に関連する。

【0002】

【従来の技術】情報技術の発展とともに、ビジネス企業体は益々増大するストレージ容量が必要になっている。平均的フォーチュン1000企業においては、来るべき年には、倍以上のストレージ容量が必要になると予想されている。加えて、容量の増大は熟練した情報技術者の不足をもたらしている。このため、多くの企業は、情報技術への投資の拡大を余儀なくさせられている。

【0003】容量の急激な増大要求に対抗するため、ストレージ管理を次第に外部委託する企業が増加している。SSP (Storage Service Provider)は、ビジネス企業体に提供できるストレージ管理サービスのひとつになっている。SSPに委ねることにより、企業体はSSPサービス提供者より必要に応じてストレージ資源を得ることが出来る。

【0004】SSPはストレージ管理サービスを提供するのみならず、ストレージシステムを自ら所有して、ユーザのホストシステムが使用するためのストレージ容量をも提供する。ユーザはSSPとの間のSLA (Service Level Agreement)契約に従って、ストレージ使用と管理サービスの為の支払いをする。

【0005】

【発明が解決しようとする課題】現在のSSP技術により、そこそこの便益は期待できるものの、更なる改良の余地が存在する。例えば、現状の慣用的なSSP技術によれば、SSPは、SSPサイトでSSPが所有しているディスクストレージシステムのストレージ資源を、ユーザサイトのホストシステムの為に提供する。

【0006】しかしながら、SSPユーザによっては、自らの装置をSSPサイトより遠隔地に設置する事を望むかもしれない。例えば、ユーザはSSP内のストレージシステムに保持されているデータを、インターネットまたは他のネットワークを通してアクセスしてもよい。さらに、セキュリティが、ユーザ及びSSP双方にとって重要な懸案事項である。ユーザにとっては、この事は、貴重なビジネス情報資産がストレージ内のデータに対するアクセスを制限することにより守られることを意味する。

【0007】SSPにとっては、この事は、データの正当性が各顧客に対して保証され、ユーザが認証されないアクセスを受けることはない、ということの意味する。例えば、大会社の各部門では、他の部門からアクセスされ

得る。真に要求される技術は、ストレージ資源へのアクセスを管理するための改良された技術である。

【0008】

【課題を解決するための手段】本発明は、ストレージ資源へのアクセスを管理する技術を提供する。本発明の実施により、ユーザは仮想アドレスと仮想ボリューム識別子のシステムを用いてストレージデバイス内の資源にアクセスできるようになる。本発明の実施により、たとえば企業体を含めてユーザが、インターネットまたは他の種類のネットワーク接続を経由して、ユーザのネットワークでSSP (Storage Service Provider)内のボリュームを使用することが可能になる。

【0009】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシーを確立することができる。

【0010】本発明の代表的な実施では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、外部ネットワークに接続するための少なくとも1つのポートを持つゲートウェイと、情報を記憶し各々1つ以上のボリュームから構成される1台以上のデバイス、サーバー、スイッチ、及び該ゲートウェイ、該サーバー、該スイッチ、および該情報を記憶する1台以上のデバイスを接続する内部ネットワークで構成される。

【0011】ゲートウェイはデータパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する1台以上のデバイスの特定の1台を指定する受信アドレスをメモリより読み出し、該データパケットの該仮想受信アドレスをメモリから読み出した対応する受信アドレスで置き換える。

【0012】実施例では、仮想受信アドレスと受信アドレスは、テーブルに格納されている。しかしながら、別の実施例としては、これらのアドレスは、ボリューム識別子、ユーザ識別子と共に、他のタイプのデータ構造、例えば、リンクリスト、キュー、スタック等に格納されても良い。さらに、このようなデータ構造は、メモリに配置されても、ディスクストレージなどに格納されても良い。

【0013】実施例によっては、ゲートウェイは、データパケット内のユーザアドレスに基づいてデータパケットの発信元の認証を行う。ある実施例では、外部ネットワークは、VPN (Virtual Private Network)機能を有する。このような実施例においては、例えば、ゲートウェイがデータパケットに対するVPN処理を実行する。

【0014】実施例によっては、外部ネットワークは第1のプロトコルを使用し、内部ネットワークは第1のプロトコルとは異なる第2のプロトコルを使用する。このような場合は、例えば、ゲートウェイが、データパケットを第1のプロトコルから第2のプロトコルに変換す

る。第1のプロトコルは、たとえばIPプロトコル、ATM、及びファイバチャネルのどれでも、または本分野の技術者であれば公知の他のタイプのプロトコルでも構わない。同様に、第2のプロトコルは、上記のプロトコルのどれかである。

【0015】実施例によっては、ゲートウェイは、データパケットを検索してコマンドと仮想プライベートボリューム識別子を検出し、検出されれば、メモリを検索して該仮想プライベートボリューム識別子に対応するボリューム識別子を見つけて、該データパケット内の該仮想プライベートボリューム識別子を該ボリューム識別子で置き換える。

【0016】実施例によっては、ゲートウェイは、外部ネットワークに送信されるデータパケットを受け取り、メモリを検索して該データパケットより抽出された受信アドレスを検出し、メモリから対応する仮想受信アドレスを読み込み、該データパケット内の該受信アドレスをメモリから読み込んだ対応する仮想受信アドレスで置き換える。

【0017】本発明の他の実施例では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも1つのポートを持つサーバー、情報を記憶し各々が1つ以上のボリュームで構成される1台以上のデバイス、スイッチ、及び該サーバー、該スイッチ、該情報を記憶する1台以上のデバイスを接続する内部ネットワークで構成される。

【0018】該サーバーは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する1台以上のデバイスの特定の1台を指定する受信アドレスをメモリから読み込み、該データパケットの該仮想受信アドレスをメモリから読み込んだ対応する受信アドレスで置き換える。

【0019】本発明の他の実施例では、ストレージ装置が提供される。本ストレージ装置は、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも1つのポートを持つスイッチと、情報を記憶し各々が1つ以上のボリュームで構成される1台以上のデバイス、サーバー、及び該サーバー、該スイッチ、該情報を記憶する1台以上のデバイスを接続する内部ネットワークで構成される。

【0020】該スイッチは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する1台以上のデバイスの特定の1台を指定する受信アドレスをメモリから読み込み、該データパケットの該仮想受信アドレスをメモリから読み込んだ対応する受信アドレスで置き換える。

【0021】本発明の他の実施例では、ゲートウェイは、外部ネットワークに接続する第1のプロトコルを使用し、内部ネットワークに接続する第2のプロトコルを使用する。このような場合は、例えば、ゲートウェイが、データパケットを第1のプロトコルから第2のプロトコルに変換する。

が提供される。本ストレージ装置は、情報を記憶し各々が1つ以上のボリューム、プロセッサ、メモリ、および外部ネットワークに接続するための少なくとも1つのポートから構成される1台以上のデバイス、スイッチ、サーバー、及び該サーバー、該スイッチ、および該情報を記憶する1台以上のデバイスを接続する内部ネットワークで構成される。

【0022】該情報を記憶する1台以上のデバイスは、データパケットを受信しこれを記憶し、メモリを検索して該データパケットより抽出した仮想受信アドレスを検出し、該仮想受信アドレスに対応し情報を記憶する1台以上のデバイスの特定の1台を指定する受信アドレスをメモリから読み出し、該データパケットの該仮想受信アドレスをメモリから読み出した対応する受信アドレスで置き換える。

【0023】本発明の代表的な実施例では、ストレージを管理する方法が提供される。本方法は、データパケットを受信し、該データパケットより仮想受信アドレスを抽出し、該仮想受信アドレスに対応する情報を記憶する1台以上のデバイスの特定の1台を指定する受信アドレスをメモリから読み出し、該データパケットの該仮想受信アドレスを該対応する受信アドレスで置き換えることを含む。

【0024】本発明により、慣用的技術に勝る数々の便益が実現される。本発明の実施により、企業体を含めてユーザが、インターネット、または他の種類のネットワーク接続を経由して、ユーザのネットワークで、SSP (Storage Service Provider)内のボリュームを使用することが可能になる。

【0025】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシーを確立することができる。各種の便益が本明細書で述べられている。本発明の更なる本質と便益は、本明細書のこれからの部分と添付図面を参照することにより、明らかになる。

【0026】

【発明の実施の形態】本発明は、ストレージ資源へのアクセスを管理する技術を提供するものである。本発明により、ユーザは、ストレージデバイスの仮想アドレスと仮想ボリューム識別子(ID)のシステムを用いてストレージ資源へアクセス出来るようになる。本発明の実施により、SSP (Storage Service Provider)は、インターネットまたは他の種類のネットワーク接続を通して、例えば企業体も含めて、ユーザのネットワークでユーザに対してボリュームを利用可能にする。

【0027】本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、及び装置の固有情報を隠蔽し、双方

al Private Network)は、インターネットのようなパブリックネットワークを用いて、プライベートネットワーク環境を実現する為のネットワーク技術である。

【0028】VPNを使用して、2つ以上のネットワークがインターネットを通して接続でき、1つのプライベートネットワークとして互いに通信できるようになる。現状の慣用的VPN技術の注目すべき限界の1つは、VPNを構成するネットワーク機器のすべての固有情報を隠蔽するものではないことである。

【0029】ゾーン技術は、FC (Fibre Channel)スイッチで採用されている技術である。ゾーン技術では、1つのポートを他のポートに割り当て可能にし、1つのポートに接続されている装置が、自ポートに割り当てられるべき他のポートに接続されているボリュームを使用出来るようにする。通常は、各装置は直接FCスイッチに接続される。

【0030】さらに、慣用的なゾーン技術では、共通のポートに接続され、他の装置から使用されてしまう可能性があるボリュームの固有情報を隠蔽しない。LUN (Logical Unit Number)セキュリティは、例えば、ファイバチャネルで接続されたストレージデバイスがWWN (World Wide Names)と呼ばれる装置の固有情報を検出し、ストレージデバイス内のボリュームの固有情報を不当アクセスから保護するストレージ技術である。通常は、各装置は直接FCスイッチに接続される。さらに、慣用的な手法では、ユーザはLUNとポートアドレスを認識するだろう。

【0031】図1は、本発明の一実施例でのSSP (Storage Service Provider)の代表的な構成を示す図である。グループA1001は、ユーザのローカルネットワークを示している。グループB1007は、もう一つのユーザのローカルネットワークを示している。クライアントC1006は、個人ユーザを示している。データセンタ1013は、実施例では、SSPに相当するストレージプロバイダの装置で構成される。データセンタ1013は、少なくとも1つのゲートウェイ1014と少なくとも1つのストレージ1038を有する。

【0032】ユーザはWAN (Wide Area Network)1012を通して、データセンタ1013に接続できる。WAN1012は、例えば、インターネットやATMリース回線などである。各ユーザは、例えば、同じネットワークを使用してデータセンタ1013に接続できる。ユーザは、専用のリース回線を使用してデータセンタ1013に直接接続することもできる。ゲートウェイ1014は、データセンタ1013外のネットワーク1012に接続する為の少なくとも1つのポート1017を有する。

【0033】ゲートウェイ1014は、データセンタ1013内のネットワーク1025に接続する為の少なくとも1つのポート1018を有する。ネットワーク1025は、例えば、ファイバチャネルネットワークに使用さ

れる。ストレージ1038はネットワーク1025と接続する為の少なくとも1つのポート1042を有する。ボリューム1044はストレージ1038に対して定義され、例えば、SCSI (Small Computer System Interface) プロトコルで定義されるLUN (Logical Unit Number) として使用されるボリュームIDを持つ。

【0034】ポート1043はネットワーク1045に接続され、管理の為に使用される。管理ターミナル1036はストレージ1038、1037、1034、1035にネットワーク1045経由で接続され、ストレージ構成を定義する為に使用される。スイッチ1026はネットワーク1025に接続する為の少なくとも1つのポート1029を有する。スイッチ1026はストレージ1034に接続する為の少なくとも1つのポート1031を有する。他の実施例、例えば、ネットワーク1025とネットワーク1045が共にIPネットワークの様に同じタイプの場合は、両ネットワークは1つのネットワークとして統合されても良い。

【0035】他の実施例、例えば、ネットワーク1012がネットワーク1025と異なるネットワーク、例えば、ネットワーク1012がIPネットワークで、ネットワーク1025がFCネットワークの場合は、ゲートウェイ1014がこの異なるネットワーク間のプロトコル変換の役割を果たす。ストレージ1034が、例えば、ネットワーク1025がIPネットワークで、ネットワーク1048がFCネットワークのように異なったタイプのネットワークをサポートする実施例の場合は、スイッチ1026が両者間のプロトコル変換の役割を果たす。

【0036】このような実施例の場合は、ストレージ1034とストレージ1038は異なったネットワークプロトコルをサポートする。例えば、ネットワーク1048とネットワーク1046が異なったプロトコルをサポートし、ネットワーク1046がネットワーク1025と同じプロトコルを採用する場合は、スイッチ1026がプロトコル変換の役割を果たす。さらに、ストレージ1034とストレージ1038は異なったネットワークプロトコルをサポートし、異なったストレージアクセスプロトコルを採用する事もできる。

【0037】もう一つの実施例として、ネットワーク1048とネットワーク1046が異なったネットワークプロトコルを採用し、ストレージ1034とストレージ1035がスイッチ1026を通して通信する場合は、スイッチ1026がプロトコル変換の役割を果たす。さらに、ストレージ1034とストレージ1038は異なったネットワークプロトコルをサポートし、異なったストレージアクセスプロトコルを採用する事もある。データセンタ1013はスイッチ1026、または、サーバ1020、または双方が省略されても良い。

【0038】図2は本発明の一実施例での代表的なプログラム

例で示されるプログラムは、図1のゲートウェイ1014のメモリ1015中に展開される。図2の実施例で示されるように、通信プログラム2001は、1つ以上のVPN (Virtual Private Network) プログラム2002、認証プログラム2003、ビュープログラム2004、プロトコル変換プログラム2005、及び送受信プログラム2006を含む複数の要素プログラムプロセスで構成される。

【0039】VPN プログラム2002は、ユーザがパブリックネットワークを使用してデータセンタ1013内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない場合は、VPN プログラム2002は省略可能である。認証プログラム2003は、データセンタ1013内のストレージデバイス1034内の情報にアクセスしようとしているユーザの認証を可能とする。

【0040】ゲートウェイ1014がユーザ認証を行わない場合は、認証プログラム2003は省略可能である。ビュープログラム2004は、データセンタ1013内のデータ蓄積用ボリュームに対する仮想及び実アドレスの変換を実行する。プロトコル変換プログラム2005は、例えば、IPネットワークとFCネットワークの如く、異なったトポロジのネットワークで結合された装置が互いに通信できる様に、プロトコル変換を行う。

【0041】さらに、プロトコル変換プログラム2005は、例えば、SCSIとFCの如く、異なったストレージアクセスプロトコルを持つ装置が互いに通信できる様にもする。データセンタ1013外のネットワーク1012とデータセンタ1013内のネットワーク1025が同じ種類の場合は、プロトコル変換プログラム2005は省略可能である。送受信プログラム2006はネットワークを経由した通信を司る。ビューテーブル2007は、ビュープログラム2004が利用できる様に、多様なユーザに割り当てられたデータセンタ1013内のストレージに関する情報を維持しており、メモリ1015内に展開される。

【0042】図3は、本発明の一実施例でのビューテーブルの代表的なフォーマットを示す図である。図3の実施例に示される如く、ビューテーブル2007はユーザ用の複数の情報欄により構成される。ユーザタイプ3001はユーザに関する情報を示す。ユーザアドレス3002は、個別ユーザのマシンのアドレス、または、複数ユーザのアドレスグループを示す。例えば、ユーザグループ3007のように、ユーザタイプ3001がグループにセットされている場合は、グループ3007に属するユーザは、データセンタ1013内の同一ボリュームにアクセスする共通ユーザセットのアドレス301

【0043】ユーザタイプ3001が3008の如く、“個人”にセットされている場合は、ユーザは、データセンタ1013内のボリュームにアクセスできるユーザアドレス3011で定義される。仮想受信アドレスVDA (Virtual Destination Address) 3003は、ユーザに開示されているストレージユニットを指定する為にユーザが使用するアドレスである。

【0044】ストレージデバイスは、ユーザの情報が蓄積され、ユーザに開示されているボリュームを持つ。ユーザがデータセンタ1013をアクセスするのにVPNを使用する実施例においては、VDAはVPNを使用するユーザによって定義されたプライベートネットワークでのIPアドレスである。受信アドレス3004は、データセンタ1013内のストレージデバイスのアドレスで、ユーザには開示されていない。例えば、受信アドレス3004は、IPアドレス、ホスト名、ファイバチャネルのWWN (World Wide Name) 等である。

【0045】ストレージユニットがネットワーク接続の為に2つ以上のポートを持っている場合は、各ポート毎に受信アドレス3004が定義される。仮想プライベートボリュームID3005は、ユーザがアクセスしたいボリュームを指定する為にユーザによって使用されるアドレスである。ボリュームID3006は、ユーザには開示されていないボリュームIDである。ボリュームID3006は、例えば、多くの実装例では、SCSIプロトコルで定義されるLUN (Logical Unit Number) で良い。ストレージユニットは、ボリュームID3006を用いてボリュームにアクセスする。

【0046】図4は、本発明の一実施例での代表的な通信プログラムを示すフローチャートである。図2に示される如く、本実施例では、通信プログラム2001はゲートウェイ1014内のメモリ1015に存在する。通信プログラム2001は、データセンタ1013内のボリュームのひとつに格納すべきデータを含んだデータパケットを受信し処理する。

【0047】データパケットを受信後、ステップ4001にて、パケットは、例えば、グループAのクライアント1002の様な、データセンタの外部から受信した内向きデータパケットか否かが判定される。データパケットがデータセンタ1013の外部から受信された場合は、処理はステップ4002に進み、そうでなければステップ4008に進む。データセンタ1013との接続にVPNを使用する場合は、オプションステップ4002にて、パケットはVPNプログラム2002によって処理される。

【0048】実施例によっては、VPNを使用する場合は、パブリックネットワークでデータを送信する前にデータを暗号化し、受信後に復号処理を行う。セキュリティをより確実にする為、データのみならず送受信のネッ

がって、VPNプログラム2002はデータパケットのデータに加えて追加的にアドレス情報についても復号処理を実施する。

【0049】次に、オプションステップ4003にて、認証プログラム2003によりパケットの認証確認がなされる。パケットが認証されると、処理はステップ4004に進み、そうでなければ、ステップ4007にてパケットは拒絶される。オプションステップ4004にて、プロトコル変換プログラム2005が、必要なプロトコル変換をすべて実施する。例えば、データパケットフォーマット、アドレスフォーマット等が変換される。

【0050】次に、ステップ4005にて、ビュープログラム2005が、ビューテーブル2007の当該パケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。内向きパケットの場合は、仮想受信アドレスを受信アドレスに、仮想ボリュームIDをボリュームIDに置き換える。

【0051】本実施例での代表的なビュープログラムの処理例を図5に示す。ステップ4015にて、ビュープログラム2005の処理結果がチェックされる。ビュープログラムが“no good (NG)”を返した場合は、パケットはステップ4007にて拒絶され、次のパケット処理の為にステップ4001に戻る。

【0052】逆に、ビュープログラムが“no good (NG)”を返さなかった場合は、ステップ4006にて、パケットはデータセンタ内のネットワーク1025に送られ、処理は次のパケット処理の為にステップ4001に戻る。

【0053】データパケットがデータセンタ1013の外部から受信されたものではなかった場合は、ステップ4008にて、当該データパケットはデータセンタ1013の内部より外部に発信された外向きパケットか否かが判定される。当該パケットがデータセンタ1013の内部、例えばストレージ1038、から受信されたものなら、ステップ4009にて、ビュープログラム2005がビューテーブル2007内の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。

【0054】外向きパケットの場合は、受信アドレスを仮想受信アドレスに、ボリュームIDを仮想ボリュームIDに置き換える。そうでない場合は、ステップ4013にて、処理を終了して良いか、または、ステップ4014にてエラー回復処理を行ってから次のパケット処理の為にステップ4001に戻るか、を判定する。次に、必要ならオプションステップ4010にて、データパケットのプロトコル変換が実施される。

【0055】次に、VPN使用時には、オプションステップ4011にて、VPNプログラム2002がデータパケット処理を行う。VPNプログラム2002は、データパ

報についても暗号化処理を実施する。次に、ステップ4012にて、当該データパケットはデータセンタ1013の外部ネットワーク1012に送信される。VPNがサポートされていない、または使用されない実施例では、VPN処理ステップ4002と4011は省略される。

【0056】データセンタ1013の外部のネットワーク1012とデータセンタ1013の内部のネットワーク1025が同じタイプの場合、プロトコル変換処理ステップ4004と4010は省略可能である。ゲートウェイがユーザチェックを行わない場合は、認証処理ステップ4003は省略可能である。

【0057】図5は、本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。本実施例の図5で示されるビュープログラム処理は、図2のビュープログラム2004と図4のステップ4005と4009の処理に対応する。実施例では、データパケット受信後、ステップ5001にて、当該データパケットはデータセンタ1013の外部から受信された内向きデータパケットか否かが判定される。

【0058】当該データパケットがデータセンタ1013の外部からのものであれば、ステップ5012にて、ユーザによって定義され、ユーザによって使用されるストレージアドレスである仮想受信アドレス3003はユーザにとって正しいか否かが判定される。本チェックは、各ユーザの正しいアドレスを登録しているビューテーブル2007を参照することにより実施される。

【0059】実施例では、仮想受信アドレス3003は、当該データパケットを送信したユーザに対して正しいアドレスか否かがチェックされる。仮想受信アドレス3003が正しくなければ、処理は、“no good (NG)”応答を呼び出したプロセスに返す。正しい場合は、ステップ5002にて、図3のビューテーブル2007を検索して当該データパケット内の仮想受信アドレス3003に対応する受信アドレス3004を求める。

【0060】次に、ステップ5003にて、当該データパケット内の仮想受信アドレス3003をビューテーブル2007から求めた受信アドレス3004に置き換える。次に、ステップ5004にて、当該データパケットはストレージアクセスコマンドを含むか否か、また含むなら仮想ボリュームID3005を含むかが判定される。当該データパケットが仮想ボリュームIDを含まなければ、当該データパケットにおいて仮想受信アドレス3003を受信アドレス3004に変換した状態で、OK状態の応答を呼び出したプロセスに返す。

【0061】仮想ボリュームIDを含めば、ステップ5013にて、再度ビューテーブル2007をチェックして、仮想プライベートボリュームIDがデータパケットを送信したユーザに対して正しいか否かが判定される。仮想プライベートボリュームIDが正しくなければ、処理は“no good (NG)”応答を呼び出したプロセスに返す。正

しい場合は、ステップ5005にて、ビューテーブル2007を検索して、当該データパケットを送信したユーザに対する仮想プライベートボリュームID3005を求める。次に、ステップ5006にて、当該データパケット内の仮想プライベートボリュームID3005をビューテーブル2007から求めたボリュームID3006に置き換える。

【0062】データパケットがデータセンタ1013の外部から受信したものでなければ、本パケットは外向きパケットである。したがって、ステップ5007にて、ビューテーブル2007を検索して当該データパケットの受信ユーザに対応する仮想受信アドレス3003を求める。

【0063】次に、ステップ5008にて、当該データパケット内の受信アドレス3004をビューテーブル2007より抽出したユーザ用の仮想受信アドレス3003に置き換える。次に、判定のステップ5009にて、当該データパケットはストレージアクセスコマンドとボリュームID3006を含むかが判定される。当該データパケットがストレージアクセスコマンドを含み、当該コマンドがボリュームID3006を含むなら、ステップ5010にて、ビューテーブル2007を検索して当該ユーザのボリュームID3006を求める。ステップ5011にて、ボリュームID3006をビューテーブル2007より抽出したユーザ用の対応する仮想ボリュームID3005に置き換える。

【0064】当該データパケットがストレージアクセスコマンドとボリュームIDを含まなければ、ユーザに対する受信アドレスを仮想受信アドレスに変換した状態で、OK状態の応答を呼び出したプロセスに返す。ゲートウェイ1014がボリュームIDを扱わない場合は、ステップ5004、5005、5006、5009、5010、5011、及び5013は省略可能である。

【0065】図6は、本発明の一実施例でのユーザに見える代表的なストレージシステムの図である。図6に示すように、データセンタ1013は情報を記憶するための複数のボリュームを有する。例えば、これらのボリュームは、1034、1037、1038等の複数のストレージユニットより割り当てられる事が出来る。複数のユーザは、1つ以上のネットワーク1012を使用してデータセンタ1013に接続することにより、データセンタ1013内の多様なボリューム上の情報にアクセスする。

【0066】例えば、グループA 1001のユーザは、仮想受信アドレス6001を用いて、WAN1012を通して、データセンタ1013に接続する。グループA 1001には、彼らのストレージは仮想ボリューム6002のイメージとして表われる。グループB 1007の他のユーザは、仮想受信アドレス6005を用いて、WAN1012を通して、データセンタ1013に接続する。

【0067】同様に、グループB 1007には、彼らのストレージは、仮想ボリューム6006のイメージとして表われる。個人ユーザのクライアントC 1006は、仮想受信アドレス6003を用いて、WAN1012を通して、データセンタ1013に接続する。ユーザC 1006には、彼らのストレージは仮想ボリューム6004のイメージとして表われる。

【0068】したがって、データセンタ1013は、各ユーザに対して独立の個別のボリュームがある様に見える。さらに、各ユーザは、データセンタ1013内の他のユーザのストレージボリュームを見ることは出来ない。

【0069】図7は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図7の実施例では、プログラムは、図1のサーバー1020内のメモリ1022内に展開される。図7の実施例で示されるように、通信プログラム2001は、1つ以上のVPN (Virtual Private Network) プログラム2002、認証プログラム2003、ビュープログラム2004、プロトコル変換プログラム2005、及び送受信プログラム2006を含む複数の要素プログラムプロセスで構成される。VPN プログラム2002は、ユーザがパブリックネットワークを使用してデータセンタ1013内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。

【0070】ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム2002は省略可能である。認証プログラム2003は、データセンタ1013内のストレージデバイス1034内の情報にアクセスしようとしているユーザの認証を可能とする。サーバー1020がユーザ認証を行わない場合は、認証プログラム2003は省略可能である。ビュープログラム2004は、データセンタ1013内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。

【0071】プロトコル変換プログラム2005は、例えば、SCSIとFCの様に、異なったストレージアクセスプロトコルを持つ装置が互いに通信できる様にするプロトコル変換機能を有する。ユーザ装置とデータセンタ1013内のストレージ装置が、同じ種類のストレージアクセスプロトコルを持つ場合は、プロトコル変換プログラム2005は、省略可能である。

【0072】たとえば、ネットワーク1012がIPネットワークプロトコルで、ネットワーク1025がFCネットワークの様に、異なったネットワークプロトコルを使用している場合は、ゲートウェイ1014が異なったタイプのネットワークプロトコル間のプロトコル変換を行う。実施例では、データは、データセンタ1013の外部からゲートウェイ1014を経由して受信され、ゲートウェイ1014がデータセンタ1013内のストレージに送られる。

信される。

【0073】送受信プログラム2006は、ネットワークを経由した通信機能を提供する。ビュープログラム2007は、ビュープログラム2004が利用できる様に、多様なユーザに割り当てられたデータセンタ1013内のストレージに関する情報を維持しており、サーバー1020内のメモリ1022に展開される。図7に示した実施例では、ユーザは、図6に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【0074】図8は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図8の実施例では、プログラムは、図1のスイッチ1026内のメモリ1028に展開される。図8の実施例で示されるように、通信プログラム2001は、1つ以上のVPN (Virtual Private Network) プログラム2002、認証プログラム2003、ビュープログラム2004、プロトコル変換プログラム2005、及び送受信プログラム2006を含む複数の要素プログラムプロセスで構成される。

【0075】VPN プログラム2002は、ユーザがパブリックネットワークを使用してデータセンタ1013内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム2002は省略可能である。認証プログラム2003は、データセンタ1013内のストレージデバイス1034内の情報にアクセスしようとしているユーザの認証を可能とする。

【0076】スイッチ1026がユーザ認証を行わない場合は、認証プログラム2003は省略可能である。ビュープログラム2004は、データセンタ1013内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。プロトコル変換プログラム2005は、例えば、IPネットワークとFCネットワークの様に、異なったトポロジのネットワークで接続された装置が互いに通信できる様にするプロトコル変換機能を実行する。

【0077】さらに、プロトコル変換プログラム2005は、例えば、SCSIとFCの様に、異なったストレージアクセスプロトコルを持つ装置が互いに通信できる様にもする。データセンタ1013外のネットワーク1012とデータセンタ1013内のネットワーク1025が、同じ種類の場合は、プロトコル変換プログラム2005は省略可能である。

【0078】実施例では、データは、データセンタ1013の外部からゲートウェイ1014を経由して受信され、ゲートウェイ1014を経由して外部ターゲットに送信される。ネットワーク1012とネットワーク1025が異なったプロトコルを使用している場合は、ゲートウェイ1014がデータセンタ1013内のストレージに送られる。

実施例では、スイッチ１０２６が受信アドレスで定義されたポートにパケットを送信する。

【００７９】送受信プログラム２００６は、ネットワークを経由した通信機能を提供する。ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、スイッチ１０２６内のメモリ１０２８に展開される。図８に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【００８０】図９は、本発明の一実施例での代表的なプログラムのブロックダイアグラムである。図９の実施例では、プログラムは、図１のストレージデバイス１０３８内のメモリ１０４０に展開される。図９の実施例で示されるように、通信プログラム９００１は、１つ以上のVPN (Virtual Private Network) プログラム２００２、認証プログラム２００３、ビュープログラム９００２、データＩＯプログラム９００３、及び送受信プログラム２００６を含む複数の要素プログラムプロセスで構成される。VPN プログラム２００２は、ユーザがパブリックネットワークを使用してデータセンタ１０１３内のボリュームにアクセスするのにプライベートネットワークを定義できる様にする。

【００８１】ユーザが、パブリックネットワークを使用してプライベートネットワークを定義するためのVPNを使用しない実施例では、VPN プログラム２００２は省略可能である。認証プログラム２００３は、データセンタ１０１３内のストレージデバイス１０３８内の情報にアクセスしようとしているユーザの認証を可能とする。ストレージデバイス１０３８がユーザ認証を行わない場合は、認証プログラム２００３は省略可能である。

【００８２】ビュープログラム９００２は、データセンタ１０１３内のデータ蓄積用ボリュームの仮想及び実アドレスの変換を実行する。データＩＯプログラム９００３は、ストレージデバイス１０３８に対する情報の読み書き動作を提供する。送受信プログラム２００６は、ネットワークを経由した通信機能を提供する。

【００８３】ビューテーブル２００７は、ビュープログラム２００４が利用できる様に、多様なユーザに割り当てられたデータセンタ１０１３内のストレージに関する情報を維持しており、ストレージデバイス１０３８内のメモリ１０４０に展開される。図９に示した実施例では、ユーザは、図６に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。

【００８４】図１０は、本発明の一実施例での代表的な通信プログラムのフローチャートである。図９で示した様に、実施例では、通信プログラム９００１は、ストレージデバイス１０３８内のメモリ１０４０に展開され、通信プログラム９００１は、データセンタ１０１３

内のボリュームのひとつに蓄えられるべきデータを保有したデータパケットを受信し処理する。データパケットを受信後、ステップ１０００１にて、パケットは、例えば、グループＡのクライアント１００２の様な、データセンタの外部から受信した内向きデータパケットか否かを判定する。

【００８５】データパケットがデータセンタ１０１３の外部から受信した場合は、処理はステップ１００１０に進み、そうでなければステップ１００１１に進む。データセンタ１０１３との接続にVPNを使用する場合は、オプションステップ１００１０にて、パケットはVPNプログラム２００２によって処理される。VPNを使用する実施例では、パブリックネットワークでデータを送信する前にデータを暗号化し、受信後に復号処理を行う。セキュリティをより確実にする為、データのみならず送受信のネットワークアドレスについても暗号処理を適用する。

【００８６】したがって、VPNプログラム２００２はデータパケットのデータに加えて、追加的にアドレス情報についても復号処理を実施する。次に、オプションステップ１０００２にて、認証プログラム２００３により、パケットの認証確認がなされる。パケットが認証されると、処理はステップ１０００３に進む。そうでなければ、ステップ１０００７にてパケットは拒絶される。ステップ１０００３にて、ビュープログラム９００２が、ビューテーブル２００７の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。内向きパケットの場合は、仮想ボリュームIDをボリュームIDに置き換える。

【００８７】本実施例での代表的なビュープログラムの処理例を図１１に示す。ステップ１００１２にて、ビュープログラム９００２の処理結果がチェックされる。ビュープログラム９００２が“no good (NG)”を返した場合は、パケットはステップ１０００７にて拒絶され、次のデータパケット処理の為にステップ１０００１に戻る。逆に、ビュープログラム９００２が“no good (NG)”を返さなかった場合は、ステップ１０００４にて、データＩＯ処理が実施される。

【００８８】データＩＯプログラム９００３は、ストレージアクセスコマンドに従って、ボリュームからデータパケットへのRead処理か、データパケットからボリュームへのWrite処理かを実行する。データＩＯ処理の完了後、次のデータパケット処理のためにステップ１０００１に戻る。

【００８９】ステップ１０００１にて、データパケットがデータセンタ１０１３の外部から受信されたものではなかった場合は、ステップ１００１１にて、当該データパケットはコマンドまたはデータを送信しているデータＩＯプログラム９００３から発信されたものか否かが判定される。データパケットがデータＩＯプログラム９００３

によって発信されたものなら、ステップ10005にて、ビュープログラム9002が、ビューテーブル2007の当該データパケット発信者のエントリにしたがって、データパケット内のアドレスとボリューム情報の変換を行う。外向きパケットの場合は、ボリュームIDを仮想ボリュームIDに置き換える。

【0090】次に、ステップ10006にて、当該データパケットはデータセンタの外部に送信され、処理はステップ10001に戻って、次のデータパケット処理に備える。データパケットがデータIDプログラム9003から送られたのではない場合は、ステップ10008にて、処理を終了して良いかを判定する。処理を終了する判定の場合は、処理を終了し、そうでない場合は、ステップ10009にて、エラー回復処理を実施した後に、ステップ10001に戻って次のデータパケット処理が実施される。ストレージデバイス1038がユーザ認証を行わない場合は、認証ステップ10002は省略可能である。

【0091】図11は、本発明の一実施例での代表的なビュープログラム処理のフローチャートである。実施例において、図11のフローチャートで示したビュープログラム処理は、図9のビュープログラム9002と図10の処理ステップ10003及び10005に対応する。データパケット受信後、ステップ11001にて、本データパケットはデータセンタ1013より送信される外向きデータパケットか否かが判定される。

【0092】本データパケットが外部からデータセンタ1013に向かうものなら、処理はステップ11002に進み、逆の場合は、ステップ11005に進む。次に、ステップ11002にて、本データパケットがストレージアクセスコマンドを有するか、有する場合は、本コマンドは仮想ボリュームID3005を含むか否かが判定される。本データパケットが仮想ボリュームIDを含まなければ、処理はOK応答を伴って呼び出したプロセスに戻る。

【0093】仮想ボリュームIDを含む場合は、ステップ11009にて、ビューテーブル2007の内容をチェックして、当該仮想プライベートボリュームIDが当該パケットの送信ユーザに対して正しいか否かが判定される。不正仮想プライベートボリュームIDが検出されたら、処理は“no good”応答を呼び出したプロセスに戻す。仮想ボリュームIDが正当な場合は、ステップ11003にて、ビューテーブル2007を検索してパケット送信ユーザの仮想プライベートボリュームID3005に対応するボリュームID3006を求める。次に、ステップ11004にて、本データパケット内の仮想ボリュームID3005をビューテーブル2007から抽出したボリュームID3006により置き換える。

【0094】本データパケットがデータセンタ1013の外部から発信されたものではない場合は、本データパ

ケットは外向きパケットである。従って、判定ステップ11005にて、本データパケットはストレージアクセスコマンドとボリュームID3006を有するかをチェックする。

【0095】本データパケットがストレージアクセスコマンドを有し、本コマンドがボリュームID3006を有する場合は、ステップ11006にて、ビューテーブル2007を検索して当該ユーザのボリュームID3006を検出する。ステップ11007にて、ボリュームID3006は、ビューテーブル2007よりユーザに対応して抽出した仮想ボリュームID3005に置き換えられる。本データパケットがストレージアクセスコマンドとボリュームIDを含まない場合は、当該ユーザの受信アドレスを仮想受信アドレスに変換して、“OK”応答を呼び出したプロセスに返す。

【0096】図11に示した実施例では、ユーザは、図6に示される様なデータセンタストレージの代表的なユーザイメージを持つことが出来る。本発明のその他の実施例として、データセンタ内のゲートウェイ、サーバー、スイッチ、ストレージのような如何なる装置でも、同時にビュー変換機能を果たす事が出来る。

【0097】これまで述べたことは、本発明の好適な実施例である。付記されている請求の範囲で定義された本発明の範囲を逸脱する事なく、変更と修正が可能である事は言うまでもない。

【0098】

【発明の効果】本発明の実施により、ユーザは、仮想アドレスと仮想ボリューム識別子のシステムを用いて、ストレージデバイス内の資源にアクセスできるようになる。本発明の実施により、企業体を含めてユーザが、インターネットまたは他の種類のネットワークを経由して、ユーザのネットワークでSSP (Storage Service Provider) 内のボリュームを使用することが可能になる。本発明の実施により、SSPとユーザは、ユーザのデータセンタのみならずSSP内のストレージデバイス、ボリューム、および機器の固有情報を隠蔽し、双方にとってプライバシーを確立することができる。

【図面の簡単な説明】

【図1】本発明の一実施例でのSSP (Storage Service Provider)の代表的な構成を示すダイアグラムである。

【図2】本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。

【図3】本発明の一実施例でのビューテーブルの代表的なフォーマットを示す図である。

【図4】図4は、本発明の一実施例での代表的な通信プログラムを示すフローチャートである。

【図5】本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。

【図6】本発明の一実施例でのユーザに見える代表的な

【図 7】 本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。

【図 8】 本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。

【図 9】 本発明の一実施例での代表的なプログラムを示すブロックダイアグラムである。

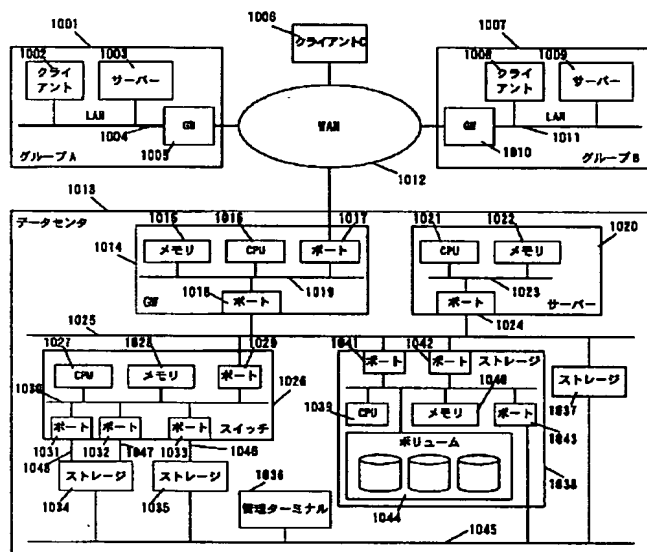
【図 10】 本発明の一実施例での代表的な通信プログラムを示すフローチャートである。

【図 11】 本発明の一実施例での代表的なビュープログラム処理を示すフローチャートである。

【符号の説明】

【図 1】

【図 1】



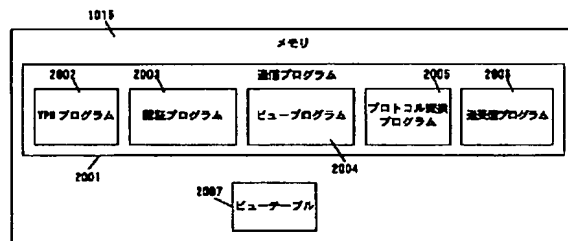
【図 3】

【図 3】

	3002	3003	3004	3005	3006
3001 ユーザタイプ	ユーザアドレス	従業員アドレス	受信アドレス	顧客プライベートボリュームID	ボリュームID
3007 グループ (256)	AAA.AA.0.0 M10	AAA.AA.1.1 M13	VPN M16	5 M19	25 M22
3008 個人	123.456.78.9 M11	123.456.78.0 M14	XIV M17	6 M20	8 M23
3009 グループ (256)	CCC.CC.0.0 M12	CCC.CC.1.1 M15	VPN M18	7 M21	24 M24
2007					

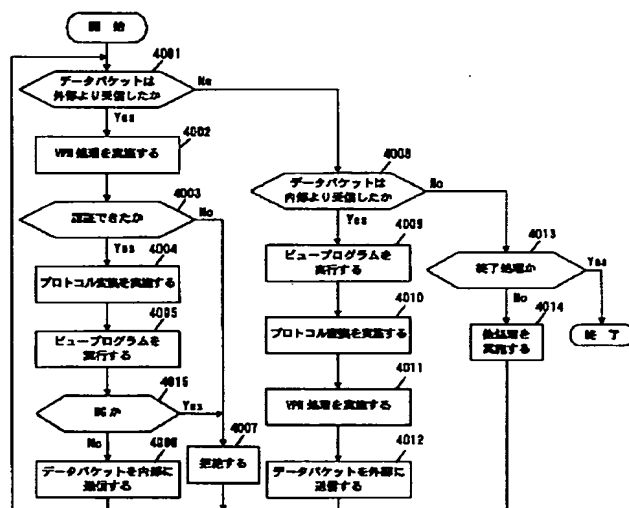
【図 2】

【図 2】



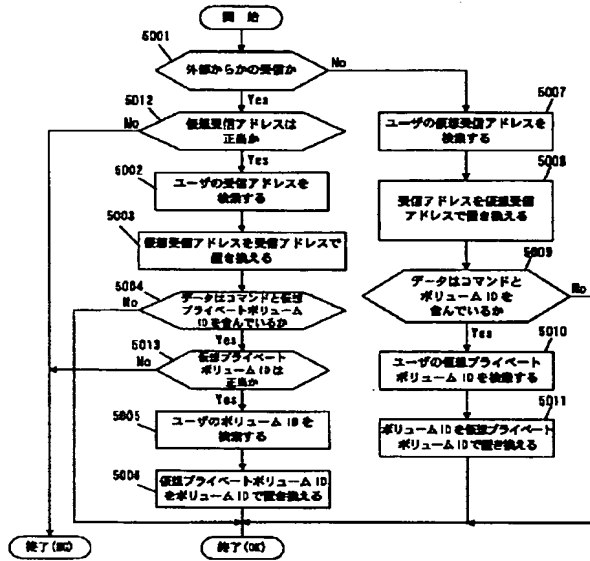
【図 4】

【図 4】



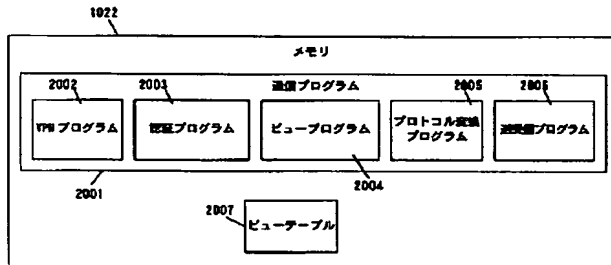
【図5】

【図5】



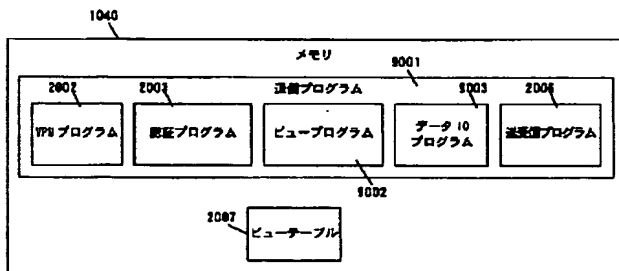
【図7】

【図7】



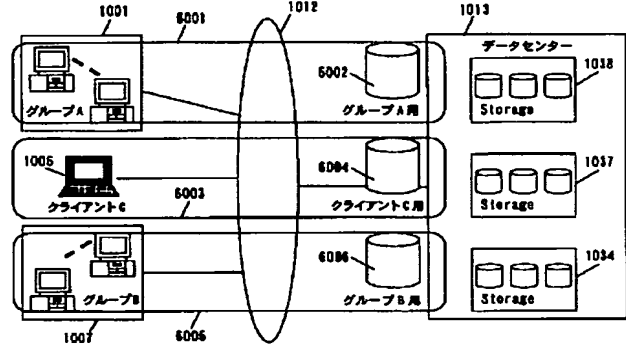
【図9】

【図9】



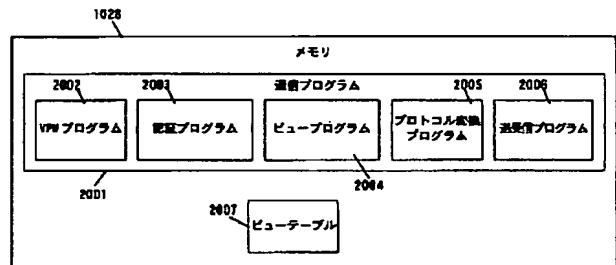
【図6】

【図6】



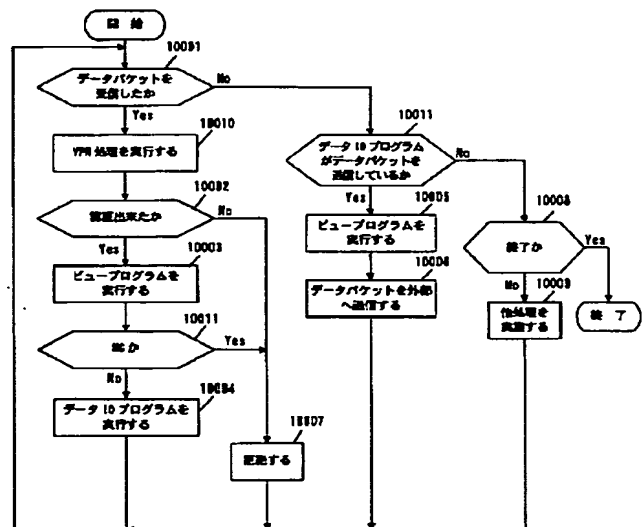
【図8】

【図8】



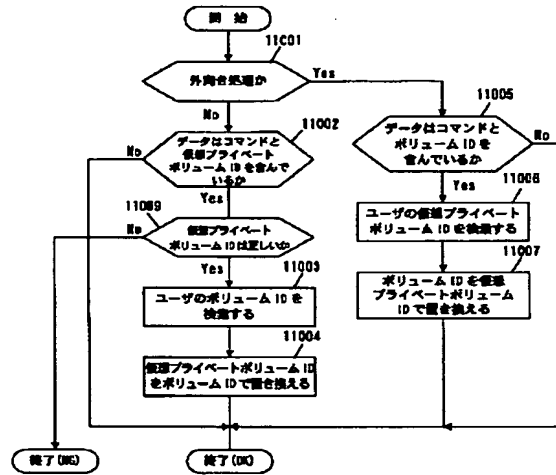
【図10】

【図10】



【図 11】

図 11



Virtual Private Volume Method and System

BACKGROUND OF THE INVENTION

10 The present invention relates generally to data storage systems, and in particular to techniques for controlling storage access based on a designated time.

 The information technology revolution brings with it an ever increasing need for more storage capacity for business enterprises. It is expected that the average Fortune 1000 company's storage requirement will more than double in the coming years.
15 In addition, growth has brought shortages of skilled persons in the information technology field. These challenges confront many companies facing the need to expand and improve their information technology assets. Increasingly, companies are turning to outsourcing storage management as a method of coping with the need to grow capacity in view of rapidly increasing demand. Storage Service Providers (SSPs) is one such service
20 for providing storage infrastructure management to business enterprises. By subscribing to an SSP, companies can obtain needed storage resources by purchasing the services from the SSP. The SSP owns storage systems, which it uses to provide storage capacity for the users' host systems, as well as provide the storage management services. Users pay for the storage usage and management services based upon the terms of a service
25 level agreement (SLA) made between the user and the SSP.

 While certain advantages to present SSP technologies are perceived, opportunities for further improvement exist. For example, according to conventional SSP technology, the SSP provides storage resources for the host systems in the user's site in disk storage systems owned by the SSP at the site. However, some SSP users would like
30 to locate their equipment remotely from the SSP site. For example, users may wish to access data held in the storage systems of the SSP via the Internet, or other network. Further, security is an important concern to both the user and the SSP. For the user, this means that valuable business information assets can be protected by restricting access to the data in storage. For the SSP, this means that data integrity is preserved for its

customers, and that no user receives access that is not authorized. For example, various divisions or departments in a large company may wish to have their own storage resources, which are private and therefore cannot be accessed by members of other divisions or departments.

5 What is needed are improved techniques for managing access to storage resources.

SUMMARY OF THE INVENTION

10 The present invention provides techniques for managing access to storage resources. In specific embodiments, storage devices provide storage resources to users using a system of virtual addresses and virtual volume identifiers. In select specific embodiments, a storage service provider (SSP) can make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data
15 center can conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

 In a representative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a gateway, having a
20 processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or more volumes; a server; a switch; and an internal network connecting the gateway, the server, the switch, and the one or more devices that store information. The gateway receives a data packet for storing, and thereupon searches in the memory for a virtual
25 destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory. In specific
30 embodiments, the virtual destination address and the destination address are stored in a table. However, in other embodiments, these addresses, as well as volume identifiers and user identifiers may be stored in other types of data structures, such as link lists, queues, stacks, and so forth. Further, these data structures may be disposed in memory or stored in a disk storage, and the like.

In a specific embodiment, the gateway authenticates a source of the data packet based upon a user address in the data packet. In some specific embodiments, the external network comprises a virtual private network (VPN). In such embodiments, the gateway, for example, performs VPN processing for the data packet.

5 In specific embodiments, the external network uses a first protocol and the internal network uses a second protocol, which may be different from the first protocol. In such cases, the gateway, for example, translates the data packet from the first protocol to the second protocol. The first protocol can be any one of an IP protocol, ATM, and Fibre channel, protocols, for example, as well as any of a variety of other protocols
10 known to those skilled in the art. Similarly, the second protocol comprises any one of the previously mentioned protocols.

In specific embodiments, the gateway searches in the data packet for a command and a virtual private volume identifier, and if found, thereupon searches in the memory for a volume identifier corresponding to the virtual private volume identifier, and
15 thereupon replaces the virtual private volume identifier in the data packet with the volume identifier.

In specific embodiments, the gateway receives a data packet being sent to the external network, and thereupon searches in the memory for a destination address retrieved from the data packet, and thereupon reads from the memory a corresponding
20 virtual destination address from the memory, and thereupon replaces in the data packet the destination address with the corresponding virtual destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a server, having a
25 processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or more volumes; a switch; and an internal network connecting the server, the switch, and the one or more devices that store information. The server receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved
30 from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises a switch, having a processor, a memory, and at least one port operative to connect to an external network; one or more devices that store information, each of the devices further comprising one or
5 more volumes; a server, and an internal network connecting the server, the switch, and the one or more devices that store information. The switch receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory a corresponding destination address for a particular one of the one or more devices that store information, and
10 thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In an alternative specific embodiment according to the present invention, a storage apparatus is provided. The storage apparatus comprises one or more devices that store information, each of the devices further comprising one or more volumes, a
15 processor, a memory, and at least one port operative to connect to an external network; a switch; a server, and an internal network connecting the server, the switch, and the one or more devices that store information. The one or more devices that store information receives a data packet for storing, and thereupon searches in the memory for a virtual destination address retrieved from the data packet, and thereupon reads from the memory
20 a corresponding destination address for a particular one of the one or more devices that store information, and thereupon replaces in the data packet the virtual destination address with the corresponding destination address from the memory.

In a representative specific embodiment according to the present invention, a method for managing storage is provided. The method comprises receiving a data
25 packet; searching for a virtual destination address retrieved from the data packet; reading a corresponding destination address for a particular one of one or more devices that store information; and replacing in the data packet the virtual destination address with the corresponding destination address.

Numerous benefits are achieved by way of the present invention over
30 conventional techniques. Specific embodiments according to the present invention can enable a storage service provider (SSP) to make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can

conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

These and other benefits are described throughout the present specification. A further understanding of the nature and advantages of the invention
 5 herein may be realized by reference to the remaining portions of the specification and the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a diagram of a representative configuration of an example
 10 storage service provider (SSP) in a specific embodiment of the present invention.

Fig. 2 illustrates a block diagram of representative programs in a specific embodiment of the present invention

Fig. 3 illustrates a diagram of a representative format of a view table in a specific embodiment of the present invention.

15 Fig. 4 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention.

Fig. 5 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention.

20 Fig. 6 illustrates a diagram of a representative storage system as seen by a user in a specific embodiment of the present invention.

Fig. 7 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

Fig. 8 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

25 Fig. 9 illustrates a block diagram of representative programs in a specific embodiment of the present invention.

Fig. 10 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention.

30 DESCRIPTION OF THE SPECIFIC EMBODIMENTS

The present invention provides techniques for managing access to storage resources. In specific embodiments, storage devices provide storage resources to users using a system of virtual addresses and virtual volume identifiers. In select specific

embodiments, a storage service provider (SSP) can make volumes available to a user, which may be a company, for example, in the user's network via the Internet or other kinds of network connections. In specific embodiments, the SSP and the user's data center can conceal the identity of the storage devices, volumes, and equipment of the SSP, as well as that of the user's data center in order to provide privacy to both user and storage provider.

Virtual Private Network (VPN) is a network technology for obtaining private network like environments using a public network, such as the Internet. Two or more networks can connect via the Internet and communicate with each other as one private network using VPN. One noteworthy limitation to conventional VPN technologies is that they do not conceal the identity of all equipment in the networks that comprise the virtual private network.

Zoning technology is a Fibre Channel (FC) switching technology. Zoning technology enables a port to be assigned to an other port, enabling equipment connected to one port to be able to use volumes that are connected to other ports to be assigned to that port. Conventionally, each piece of equipment connects to the FC switch directly. Further, conventional zoning techniques do not conceal the identity of volumes which are connected to a common port and may be used by other equipment.

Logical Unit Number (LUN) security is a storage technology in which a storage device connected by a Fibre Channel, for example, detects equipment identities, called World Wide Names (WWN), so that the identity of volumes within the storage devices are protected from unauthorized access. Conventionally, each piece of equipment connects to the FC switch directly. Further, in conventional approaches, users may be aware of a LUN and port address.

Fig.1 illustrates a diagram of a representative configuration of an example storage service provider (SSP) in a specific embodiment of the present invention. Group A 1001 indicates a user's local network. Group B 1007 indicates another user's local network. Client C 1006 indicates a personal user. A data center 1013 comprises equipment of a storage provider, which can be an SSP, in a specific embodiment. The data center 1013 has at least one gateway 1014 and at least one storage 1038. Users can connect to data center 1013 via a wide area network (WAN) 1012. WAN 1012 can be for example, the Internet, an ATM leased line, and so on. Each user can use the same network for connecting to the data center 1013, for example. The users can use their own

leased line for connecting to the data center 1013 directory, as well. Gateway 1014 has at least one port 1017 for connecting to network 1012 outside of the data center 1013.

Gateway 1014 has at least one port 1018 for connecting to network 1025 inside of the data center 1013. Network 1025 is used for accessing storage devices. Storage 1038 has

- 5 at least one port 1042 for connecting to network 1025. Volumes 1044 are defined for the storage 1038, and have volume IDs that can be for example a Logical Unit Number (LUN) defined by the Small Computer System Interface (SCSI) protocol, for example. Port 1043 is connected to network 1045, and is used for management. Management terminal 1036 is connected to storage 1038, 1037, 1034, 1035 via network 1045, and is
- 10 used to define the storage configuration. Switch 1026 has at least one port 1029 for connecting to the network 1025. Switch 1026 also has at least one port 1031 for connecting to the storage 1034. In another specific embodiment, in which the network 1025 and network 1045 are of the same type, for example both are IP networks, network 1025 and network 1045 can be integrated into one network. In another specific
- 15 embodiment, in which the network 1012 is of a different type than network 1025, for example network 1012 is an IP network and network 1025 is a Fibre Channel (FC) network, the gateway 1014 provides a protocol exchange function between these different types of networks. In a specific embodiment in which the storage 1034 supports networks of different types, for example network 1025 is an IP network and a network
- 20 1048 is an FC network, switch 1026 provides protocol exchange functions between the different protocols. In such specific embodiments, the storage 1034 and storage 1038 support different network protocols. For example, in a specific embodiment in which network 1048 and network 1046 support different protocols, and network 1046 uses the same protocol as network 1025, the switch 1026 can provide protocol exchange functions.
- 25 Further, the storage 1034 and the storage 1038 can support different network protocols and may use different storage access protocols, as well. In another specific embodiment, in which network 1048 and network 1046 use different network protocols and the storage 1034 and the storage 1035 communicate via switch 1026, the switch 1026 can provide protocol exchange function. Further, the storage 1034 and storage 1038 can support
- 30 different network protocols and may use different storage access protocols, as well. In specific embodiments, the data center 1013 can be configured such that switch 1026, server 1020, or both are not included.

Fig. 2 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In a specific embodiment, the programs illustrated by Fig. 2 are disposed in the memory 1015 of gateway 1014 in Fig. 1. As shown by Fig. 2, in a specific embodiment, a communication program 2001 comprises a plurality of

5 component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a

10 user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific

15 embodiment in which the gateway 1014 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus connected by networks of different topologies communicate with each other, such as for example an IP network communicating with an FC network. Further, the protocol exchanger program

20 2005 enables apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment, in which network 1012, external to data center 1013, and network 1025, internal to data center 1013, are of the same kind, the protocol exchanger program 2005 may be omitted. A send and receive program 2006 provides communications functions along the network. A

25 view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1015.

Fig. 3 illustrates a diagram of a representative format of a view table in a specific embodiment of the present invention. As shown by Fig. 3, in a specific embodiment, the view table 2007 comprises a plurality of information fields for users. A

30 user type 3001 indicates information about the user. A user address 3002 indicates an address of an individual user's machine, or a group of addresses for multiple users. For example, when the user type 3001 is set to "group," such as for user group 3007, users belonging to the group 3007 are defined by a common set of user addresses 3010, which

have access to the same volume in the data center 1013. When the user type 3001 is set to "personal," such as for personal user 3008, then that user is defined by a user address 3011, which can access a volume in the data center 1013. A Virtual Destination Address (VDA) 3003 is used by the user to specify a storage unit known to the user. The storage device has a volume, also known to the user, in which the user's information is stored. In a specific embodiment in which a user uses VPN to access data center 1013, the virtual destination address (VDA) is an IP address in a private network defined by the user using VPN. A destination address 3004 is an address of a storage device in the data center 1013, which is not known to the user. For example, the destination address 3004 can be an IP address, a hostname, a World Wide Name (WNN) for a fibre channel network, and so forth. When a storage unit has more than two ports for connecting to a network, then the storage unit will have a destination address 3004 for each port. A virtual private volume ID 3005 is used by user's to specify a volume that the user wishes to access. A volume ID 3006 is a volume ID that is not known to the user. Volume ID 3006 may be, for example a Logical Unit Number (LUN) defined by the SCSI protocol in various specific embodiments. The storage unit accesses the volume using the volume ID 3006.

Fig. 4 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention. As shown in Fig. 4, in a specific embodiment, communication program 2001 resides in memory 1015 of gateway 1014. The communication program 2001 receives and processes data packets containing data to be stored on one of the volumes of the data center 1013. After a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source external to data center 4001, such as from client 1002 of Group A, for example. If the packet was received from outside of the data center 1013, then processing continues with step 4002. Otherwise, processing continues with step 4008. In an optional step 4002, the packet is processed by the virtual private network program 2002, in specific embodiments that use virtual private network to connect with data center 1013. In specific embodiments, using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Accordingly, in specific embodiments, the virtual private network program 2002 performs decryption of data, and optionally address information, in the data packet. Next, the packet may be authenticated by an

authentication program 2003 in an optional step 4003. If the packet passes authentication, then processing continues with a step 4004. Otherwise, the packet is rejected in a step 4007. In optional step 4004, the protocol exchanger program 2005 performs any protocol translation required. For example, transforming data packet format, address formats, and so forth. Then, in a step 4005, view program 2005 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For inbound packets, the virtual destination address is replaced by a destination address and virtual volume ID is replaced with a volume ID. A representative view program process is illustrated by Fig. 5 for a specific embodiment. In a step 4015, a result of view program 2005 processing is checked. If the view program returned "no good (NG)," then the packet is rejected in step 4007, and processing continues with step 4001 for the next data packet. Otherwise, if the view program did not return "no good," then in a step 4006, the packet is sent to network 1025 inside the data center, and processing continues with step 4001 for the next data packet.

If the data packet was not received from outside of the data center 1013, then in a step 4008, a check is made to determine if the data packet is outbound information received from inside the data center 1013. If the packet was received from inside the data center 1013, such as from storage 1038, for example, then in a step 4009, the view program 2005 view program 2005 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For outbound packets, destination address is replaced by a virtual destination address and volume ID is replaced with a virtual volume ID. Otherwise, in a step 4013, a decision is made whether to terminate processing, or perform an error recovery task in step 4014 prior to continuing with step 4001 for the next data packet. Then, in an optional step 4010, in a specific embodiment, the protocol of the data packet is exchanged, if needed. Then, in an optional step 4011, in a specific embodiment that uses VPN, the VPN program 2002 processes the data packet. The virtual private network program 2002 performs encryption of data, and optionally address information, in the data packet. Then, in a step 4012, the data packet is sent to network 1012 outside of data center 1013. In a specific embodiment in which VPN is not supported or is not used, the VPN processing steps 4002 and 4011 may be omitted. In a specific embodiment in which the network 1012 outside of the data center 1013 and the network 1025 inside of the data

center 1013 are of the same type, the protocol exchange steps 4004 and 4010 may be omitted. In a specific embodiment in which the gateway does not check user identity, the authentication step 4003 may be omitted.

Fig. 5 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention. In specific embodiments, view program processing illustrated by the flow chart of Fig. 5 corresponds to view program 2004 of Fig. 2, and processing of steps 4005 and 4009 of Fig. 4. In a specific embodiment, after a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source outside of data center 1013 in a step 5001. If the data packet is from a source external to the data center 1013, then in a step 5012, a determination is made whether a virtual destination address 3003, which is a user defined storage address that is known to and used by the user, is the correct address for the user. This may be performed by referring to the view program table 2007, which provides the known correct addresses for each user. In a specific embodiment, the virtual destination address 3003 is checked to see if it is the correct address for the user that sent the data packet. If the virtual destination address 3003 is not correct, then processing returns a "no good" (NG) return condition to the invoking process. Otherwise, in a step 5002, the view table 2007 of Fig. 3 is searched for a destination address 3004 corresponding to the virtual destination address 3003 embedded in the data packet. Then, in a step 5003, the virtual destination address 3003 in the data packet is replaced by the destination address 3004 from view table 2007. Then, in a step 5004, a determination is made whether the data packet includes a storage access command, and if so, whether that command includes a virtual volume ID 3005. If the data packet does not include a virtual volume ID, then processing returns to an invoking process with an OK state, having translated the virtual destination address 3003 into a destination address 3004 in the data packet. Otherwise, in a step 5013, a determination is made whether the virtual private volume ID for the user who sent the data packet is correct, again by checking the contents of the view table 2007. If an incorrect virtual private volume ID is discovered, then processing returns a "no good" return condition to an invoking process. Otherwise, in a step 5005, the view table 2007 is searched for the volume ID 3006 corresponding to the virtual private volume ID 3005 for the user who sent the packet. Then, in a step 5006, the virtual volume ID 3005 in the data packet is replaced with a volume ID 3006 retrieved from the view table 2007.

If the data packet was not received from outside of the data center 1013, then it is an outbound packet. Accordingly, in a step 5007, the view table 2007 is searched for the virtual destination address 3003 for the user to whom the data packet is being sent. Then, in a step 5008, the destination address 3004 in the data packet is replaced with a virtual destination address 3003 for the user retrieved from the view table 2007. Then, in a decisional step 5009, a determination is made whether the data packet includes a storage access command and a volume ID 3006. If the data packet includes a storage access command, and that command includes a volume ID 3006, then the view table 2007 is searched for the volume ID 3006 for the user in a step 5010. The volume ID 3006 is replaced with the corresponding virtual volume ID 3005 for the user retrieved from the view table 2007 in a step 5011. Otherwise, if the data packet does not include a storage access command and volume ID, then the processing returns an "OK" condition to an invoking process, having translated the destination address for the user into a virtual destination address and the volume ID into a virtual volume ID in the data packet. In a specific embodiment in which gateway 1014 does not handle volume ID, steps 5004, 5005, 5006, 5009, 5010, 5011, and 5013 may be omitted.

Fig. 6 illustrates a diagram of a representative storage system as seen by a user in a specific embodiment of the present invention. As shown by Fig. 6, the data center 1013 comprises a plurality of volumes for storing information. In a specific embodiment, these volumes can be allocated among a plurality of storage units, such as storage units 1034, 1037 and 1038, for example. A plurality of users access information on various volumes within data center 1013, by connecting to the data center 1013 by one or more networks 1012. For example, a user, group A 1001, connects via virtual destination address 6001 via the wide area network 1012 to data center 1013. Group A 1001 is presented with an image of their storage as a virtual volume 6002. Another user, group B 1007, connects via a virtual destination address 6005 via wide area network 1012 to the data center 1013. Similarly, group B 1007 is presented with an image of their storage as a virtual volume 6006. Individual user, client C 1006, connects via virtual destination address 6003 via the wide area network 1012 to data center 1013. User C 1006 is presented with an image of their storage as a virtual volume 6004. Accordingly, the data center 1013 appears like an individual volume to each user. Further, each user is blocked from seeing storage volumes of another user inside of data center 1013.

Fig. 7 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs illustrated by Fig. 7 are disposed in the memory 1022 of server 1024 in Fig. 1. As shown by Fig. 7, in a specific embodiment, a communication program 2001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific embodiment in which the server 1024 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment in which the user's apparatus and the storage apparatus of the data center 1013 use same kind of storage access protocol, the protocol exchanger program 2005 may be omitted. In a specific embodiment in which network 1012 and network 1025 use different network protocols, for example, network 1012 uses an IP network protocol and network 1025 uses Fibre channel, the gateway 1014 performs protocol exchange functions between these different types of network protocols. In a specific embodiment, data is received from sources external to the data center 1013 via the gateway 1014, and sent to these external targets via the gateway 1014. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1022 of server 1024. A specific embodiment, as illustrated by Fig. 7, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 8 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs

illustrated by Fig. 8 are disposed in the memory 1028 of switch 1026 in Fig. 1. As shown by Fig. 8, in a specific embodiment, a communication program 2001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 2004, a protocol exchanger program 2005 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1034 of the data center 1013. In a specific embodiment in which the switch 1026 does not check user identity, the authentication program 2003 may be omitted. A view program 2004 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A protocol exchanger program 2005 provides protocol exchange functions that enable apparatus connected by networks of different topologies communicate with each other, such as for example an IP network communicating with an FC network. Further, the protocol exchanger program 2005 enables apparatus which use different storage access protocols, such as for example, SCSI and FC, to communicate with each other. In a specific embodiment, in which network 1012, external to data center 1013, and network 1025, internal to data center 1013, are of the same kind, the protocol exchanger program 2005 may be omitted. In a specific embodiment, data is received from sources external to the data center 1013 via the gateway 1014, and sent to these external targets via the gateway 1014. In a specific embodiment in which network 1012 and network 1025 use different network protocols, gateway 1014 performs protocol exchange function. In this specific embodiment, switch 1026 sends packets to a port which is defined by the destination address. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1028 of switch 1026. A specific embodiment, as illustrated by Fig. 8, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 9 illustrates a block diagram of representative programs in a specific embodiment of the present invention. In an alternative embodiment, the programs

illustrated by Fig. 9 are disposed in the memory 1040 of storage device 1038 in Fig. 1. As shown by Fig. 9, in a specific embodiment, a communication program 9001 comprises a plurality of component program processes, including one or more of a virtual private network (VPN) program 2002, an authentication program 2003, a view program 9002, a data IO program 9003 and a send and receive program 2006. A virtual private network (VPN) program 2002 enables the user to define a private network for accessing volumes within the data center 1013 using a public network. In a specific embodiment in which a user does not use the virtual private network (VPN) for defining a private network using a public network, the VPN program 2002 may be omitted. An authentication program 2003 provides the capability to authenticate the identity of a user who attempts to access information in one of the storage devices 1038 of the data center 1013. In a specific embodiment in which the storage device 1038 does not check user identity, the authentication program 2003 may be omitted. A view program 9002 provides translation of virtual and real addresses of volumes for storing data in the data center 1013. A data IO program 9003 provides reading and writing of information to and from storage device 1038. A send and receive program 2006 provides communications functions along the network. A view table 2007, which maintains information about storage in the data center 1013 that is allocated to various users for view program 2004, is also disposed in memory 1040 of storage 1038. A specific embodiment, as illustrated by Fig. 9, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

Fig. 10 illustrates a flow chart of a representative communication program in a specific embodiment of the present invention. As shown in Fig. 10, in a specific embodiment, communication program 9001 resides in memory 1040 of storage device 1038. The communication program 9001 receives and processes data packets containing data to be stored on one of the volumes of the data center 1013. After a data packet is received, a check is made whether the data packet is an inbound data packet that was received from a source external to data center 10001, such as from client 1002 of Group A, for example. If the packet was received from outside of the data center 1013, then processing continues with step 10002. Otherwise, processing continues with step 10008. In an optional step 10010, the packet is processed by the virtual private network program 2002, in specific embodiments that use virtual private network to connect with data center 1013. In specific embodiments, using a virtual private network involves encrypting data

before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving network addresses. Accordingly, in specific embodiments, the virtual private network program 2002 performs decryption of data, and optionally address information, in the data packet. Next, the packet may be authenticated by an authentication program 2003 in an optional step 10002. If the packet passes authentication, then processing continues with a step 10003. Otherwise, the packet is rejected in a step 10007. In a step 1003, view program 9002 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For inbound packets, the virtual volume ID is replaced with a volume ID. A representative view program process is illustrated by Fig. 11 for a specific embodiment. In a step 10011, a result of view program 9002 processing is checked. If the view program 9002 returned "no good (NG)," then the packet is rejected in step 10007, and processing continues with step 10001 for the next data packet. Otherwise, if the view program 9002 did not return "no good," then in a step 10004, data IO processing is performed. Data IO program 9003 reads information from a data packet to a volume or writes information from a data packet to a volume according to a storage access command. After data IO processing, processing continues with step 10001 for the next data packet.

If in step 10001, it is determined that the data packet was not received from outside of the data center 1013, then in a decisional step 10011, a determination is made whether the data packet is from the data IO program 9003 sending a command or data. If the data packet was sent by the data IO program 9003, then, in a step 10005, a view program 9002 translates address and volume information in the data packet according to an entry for the user originating the data packet in the view table 2007. For outbound packets, the volume ID is replaced with a virtual volume ID. Then, in a step 10006, the data packet is sent outside of the data center, and processing continues with step 10001 for the next data packet. Otherwise, if the data packet was not sent by the data IO program 9003, then in a step 10008, a check is made to determine whether to terminate processing. If the decision is made to terminate processing, then the processing is terminated. Otherwise, an error recovery process is performed in a step 10009, and then processing continues with another data packet in step 10001. In a specific

embodiment in which the storage 1038 does not check user identity, authentication step 10002 may be omitted.

Fig. 11 illustrates a flow chart of a representative view program processing in a specific embodiment of the present invention. In specific embodiments, view program processing illustrated by the flow chart of Fig. 11 corresponds to view program 9002 of Fig. 9, and processing of steps 10003 and 10005 of Fig. 10. In a specific embodiment, after a data packet is received, a check is made whether the data packet is an outbound data packet that being sent from the data center 1013 in a step 11001. If the data packet is from a source external to the data center 1013, then Otherwise, processing continues with a step 11005. Then, in a step 11002, a determination is made whether the data packet includes a storage access command, and if so, whether that command includes a virtual volume ID 3005. If the data packet does not include a virtual volume ID, then processing returns to an invoking process with an OK state. Otherwise, in a step 11009, a determination is made whether the virtual private volume ID for the user who sent the packet is correct, again by checking the contents of the view table 2007. If an incorrect virtual private volume ID is discovered, then processing returns a "no good" return condition to an invoking process. Otherwise, in a step 11003, the view table 2007 is searched for the volume ID 3006 corresponding to the virtual private volume ID 3005 for the user who sent the packet. Then, in a step 11004, the virtual volume ID 3005 in the data packet is replaced with a volume ID 3006 retrieved from the view table 2007.

If the data packet was not received from outside of the data center 1013, then it is an outbound packet. Accordingly, in a decisional step 11005, a determination is made whether the data packet includes a storage access command and a volume ID 3006. If the data packet includes a storage access command, and that command includes a volume ID 3006, then the view table 2007 is searched for the volume ID 3006 for the user in a step 11006. The volume ID 3006 is replaced with the corresponding virtual volume ID 3005 for the user retrieved from the view table 2007 in a step 11007. Otherwise, if the data packet does not include a storage access command and volume ID, then the processing returns an "OK" condition to an invoking process, having translated the destination address for the user into a virtual destination address and the volume ID into a virtual volume ID in the data packet. A specific embodiment, as illustrated by Fig. 11, enables users to have the representative user image of the data center storage as illustrated by Fig. 6.

In according to other embodiment of the invention, these equipment in data center, like a gateway, server, switch, and storage, any equipment has these view change function at same time.

- 5 The preceding has been a description of the preferred embodiment of the invention. It will be appreciated that deviations and modifications can be made without departing from the scope of the invention, which is defined by the appended claims.

What is claimed is:

- 1 1. A storage apparatus comprising:
2 a gateway, having a processor, a memory, and at least one port operative to
3 connect to an external network;
4 at least one of a plurality of devices that store information, each of said
5 devices further comprising at least one of a plurality of volumes;
6 a server;
7 a switch; and
8 an internal network connecting said gateway, said server, said switch, and
9 said at least one of a plurality of devices that store information; wherein
10 said gateway receives a data packet for storing, and thereupon searches in
11 said memory for a virtual destination address retrieved from said data packet, and
12 thereupon reads from said memory a corresponding destination address for a particular
13 one of said at least one of a plurality of devices that store information, and thereupon
14 replaces in said data packet said virtual destination address with said corresponding
15 destination address from said memory.
- 1 2. The apparatus of claim 1, wherein said gateway authenticates a
2 source of said data packet based upon a user address in said data packet.
- 1 3. The apparatus of claim 1, wherein said external network comprises
2 a virtual private network (VPN), and wherein said gateway performs VPN processing for
3 said data packet.
- 1 4. The apparatus of claim 1, wherein said external network uses a first
2 protocol and said internal network uses a second protocol, and wherein said gateway
3 translates said data packet from said first protocol to said second protocol.
- 1 5. The apparatus of claim 4, wherein said first protocol comprises at
2 least one of IP protocol, ATM, and Fibre channel.
- 1 6. The apparatus of claim 4, wherein said second protocol comprises
2 at least one of IP protocol, ATM, and Fibre channel.

1 7. The apparatus of claim 1, wherein said gateway searches in said
2 data packet for a command and a virtual private volume identifier, and if found,
3 thereupon searches in said memory for a volume identifier corresponding to said virtual
4 private volume identifier, and thereupon replaces said virtual private volume identifier in
5 said data packet with said volume identifier.

1 8. The apparatus of claim 1, wherein said gateway receives a data
2 packet being sent to said external network, and thereupon searches in said memory for a
3 destination address retrieved from said data packet, and thereupon reads from said
4 memory a corresponding virtual destination address from said memory, and thereupon
5 replaces in said data packet said destination address with said corresponding virtual
6 destination address from said memory.

1 9. The apparatus of claim 1, wherein said virtual destination address
2 and said destination address are stored in a table.

1 10. A storage apparatus comprising:
2 a server, having a processor, a memory, and at least one port operative to
3 connect to an external network;
4 at least one of a plurality of devices that store information, each of said
5 devices further comprising at least one of a plurality of volumes;
6 a switch; and
7 an internal network connecting said server, said switch, and said at least
8 one of a plurality of devices that store information; wherein
9 said server receives a data packet for storing, and thereupon searches in
10 said memory for a virtual destination address retrieved from said data packet, and
11 thereupon reads from said memory a corresponding destination address for a particular
12 one of said at least one of a plurality of devices that store information, and thereupon
13 replaces in said data packet said virtual destination address with said corresponding
14 destination address from said memory.

1 11. The apparatus of claim 10, further comprising a gateway, said
2 gateway having a processor, a memory, and at least one port operative to connect to an
3 external network, and wherein said external network uses a first protocol and said internal

4 network uses a second protocol, and wherein said gateway translates said data packet
5 from said first protocol to said second protocol.

1 12. The apparatus of claim 11, wherein said first protocol comprises at
2 least one of IP protocol, ATM, and Fibre channel.

1 13. The apparatus of claim 11, wherein said second protocol comprises
2 at least one of IP protocol, ATM, and Fibre channel.

1 14. The apparatus of claim 11, wherein said external network
2 comprises a virtual private network (VPN), and wherein said gateway performs VPN
3 processing for said data packet.

1 15. The apparatus of claim 10, wherein said server searches in said
2 data packet for a command and a virtual private volume identifier, and if found,
3 thereupon searches in said memory for a volume identifier corresponding to said virtual
4 private volume identifier, and thereupon replaces said virtual private volume identifier in
5 said data packet with said volume identifier.

1 16. The apparatus of claim 10, wherein said server receives a data
2 packet being sent to said external network, and thereupon searches in said memory for a
3 destination address retrieved from said data packet, and thereupon reads from said
4 memory a corresponding virtual destination address from said memory, and thereupon
5 replaces in said data packet said destination address with said corresponding virtual
6 destination address from said memory.

1 17. The apparatus of claim 10, wherein said server authenticates a
2 source of said data packet based upon a user address in said data packet.

1 18. A storage apparatus comprising:
2 a switch, having a processor, a memory, and at least one port operative to
3 connect to an external network;
4 at least one of a plurality of devices that store information, each of said
5 devices further comprising at least one of a plurality of volumes;
6 a server; and

7 an internal network connecting said server, said switch, and said at least
8 one of a plurality of devices that store information; wherein
9 said switch receives a data packet for storing, and thereupon searches in
10 said memory for a virtual destination address retrieved from said data packet, and
11 thereupon reads from said memory a corresponding destination address for a particular
12 one of said at least one of a plurality of devices that store information, and thereupon
13 replaces in said data packet said virtual destination address with said corresponding
14 destination address from said memory.

1 19. The apparatus of claim 18, further comprising a gateway, said
2 gateway having a processor, a memory, and at least one port operative to connect to an
3 external network, and wherein said external network uses a first protocol and said internal
4 network uses a second protocol, and wherein said gateway translates said data packet
5 from said first protocol to said second protocol.

1 20. The apparatus of claim 19, wherein said first protocol comprises at
2 least one of IP protocol, ATM, and Fibre channel.

1 21. The apparatus of claim 19, wherein said second protocol comprises
2 at least one of IP protocol, ATM, and Fibre channel.

1 22. The apparatus of claim 19, wherein said external network
2 comprises a virtual private network (VPN), and wherein said gateway performs VPN
3 processing for said data packet.

1 23. The apparatus of claim 18, wherein said switch searches in said
2 data packet for a command and a virtual private volume identifier, and if found,
3 thereupon searches in said memory for a volume identifier corresponding to said virtual
4 private volume identifier, and thereupon replaces said virtual private volume identifier in
5 said data packet with said volume identifier.

1 24. The apparatus of claim 18, wherein said switch receives a data
2 packet being sent to said external network, and thereupon searches in said memory for a
3 destination address retrieved from said data packet, and thereupon reads from said
4 memory a corresponding virtual destination address from said memory, and thereupon

5 replaces in said data packet said destination address with said corresponding virtual
6 destination address from said memory.

1 25. The apparatus of claim 18, wherein said switch authenticates a
2 source of said data packet based upon a user address in said data packet.

1 26. A storage apparatus comprising:
2 at least one of a plurality of devices that store information, each of said
3 devices further comprising at least one of a plurality of volumes, a processor, a memory,
4 and at least one port operative to connect to an external network;
5 a switch;
6 a server; and
7 an internal network connecting said server, said switch, and said at least
8 one of a plurality of devices that store information; wherein
9 said at least one of a plurality of devices that store information receives a
10 data packet for storing, and thereupon searches in said memory for a virtual destination
11 address retrieved from said data packet, and thereupon reads from said memory a
12 corresponding destination address for a particular one of said at least one of a plurality of
13 devices that store information, and thereupon replaces in said data packet said virtual
14 destination address with said corresponding destination address from said memory.

1 27. The apparatus of claim 26, further comprising a gateway, said
2 gateway having a processor, a memory, and at least one port operative to connect to an
3 external network, and wherein said external network uses a first protocol and said internal
4 network uses a second protocol, and wherein said gateway translates said data packet
5 from said first protocol to said second protocol.

1 28. The apparatus of claim 27, wherein said first protocol comprises at
2 least one of IP protocol, ATM, and Fibre channel.

1 29. The apparatus of claim 27, wherein said second protocol comprises
2 at least one of IP protocol, ATM, and Fibre channel.

1 30. The apparatus of claim 27, wherein said external network
2 comprises a virtual private network (VPN), and wherein said gateway performs VPN
3 processing for said data packet.

1 31. The apparatus of claim 26, wherein said at least one of a plurality
2 of devices that store information searches in said data packet for a command and a virtual
3 private volume identifier, and if found, thereupon searches in said memory for a volume
4 identifier corresponding to said virtual private volume identifier, and thereupon replaces
5 said virtual private volume identifier in said data packet with said volume identifier.

1 32. The apparatus of claim 26, wherein said at least one of a plurality
2 of devices that store information receives a data packet being sent to said external
3 network, and thereupon searches in said memory for a destination address retrieved from
4 said data packet, and thereupon reads from said memory a corresponding virtual
5 destination address from said memory, and thereupon replaces in said data packet said
6 destination address with said corresponding virtual destination address from said
7 memory.

1 33. The apparatus of claim 26, wherein said at least one of a plurality
2 of devices that store information authenticates a source of said data packet based upon a
3 user address in said data packet.

1 34. A method for managing storage, comprising:
2 receiving a data packet;
3 searching for a virtual destination address retrieved from said data packet;
4 reading a corresponding destination address for a particular one of at least
5 one of a plurality of devices that store information; and
6 replacing in said data packet said virtual destination address with said
7 corresponding destination address.

1

1

【 1】

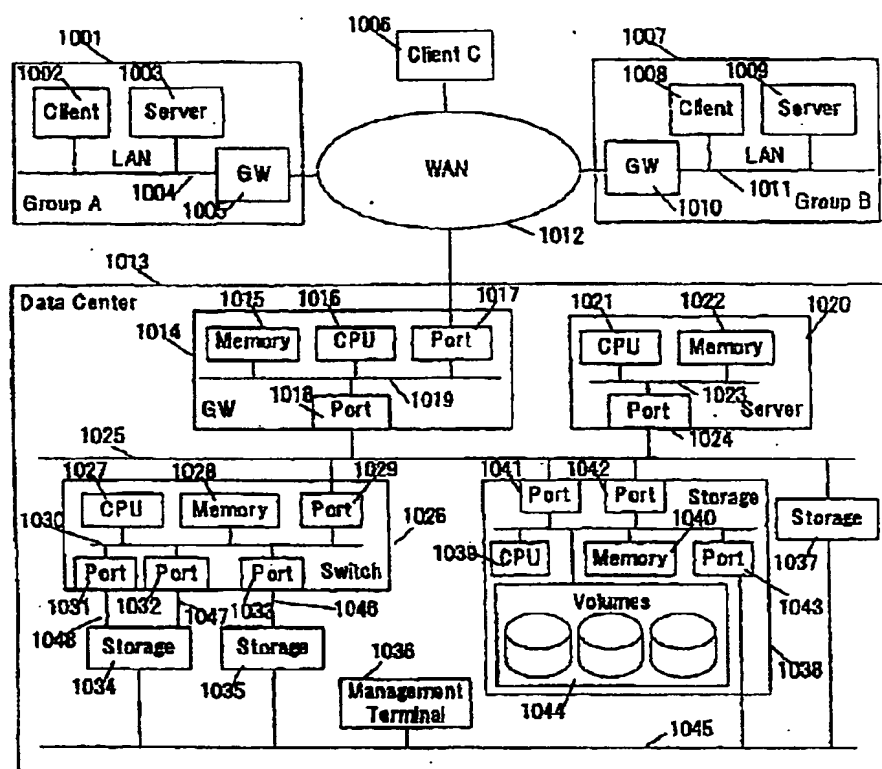


Fig 1.

【圖 2】

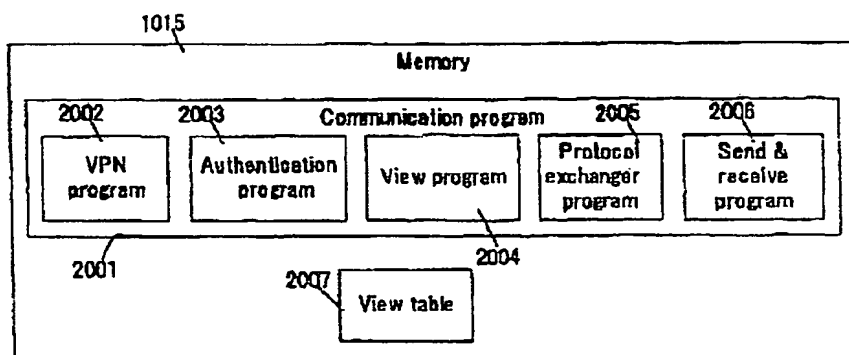


Fig 2

【 図 3 】

3001	User Type	User Address 3002	Virtual Destination Address 3003	Destination Address 3004	Virtual Private Volume ID 3005	Volume ID 3006
3007	Group	AAAAA.** 3010	AAA.AA.1.3 3013	WWN 3016	5 3019	25 3022
3008	Personal	123.456.78.9 3011	123.456.78.0 3014	XXY 3017	6 3020	8 3023
3009	Group	CCC.CC.** 3012	CCC.CC.1.3 3015	WWN 3018	7 3021	24 3024
2007	:	:	:	:	:	:

Fig. 3

【 図 4 】

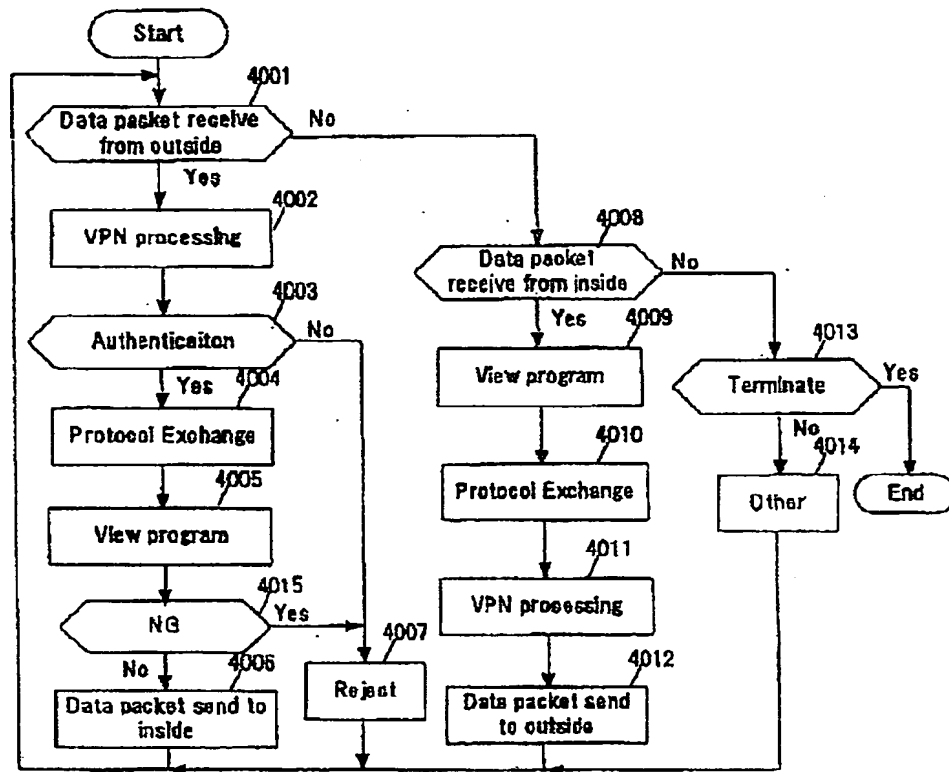


FIG. 4

【 図 5 】

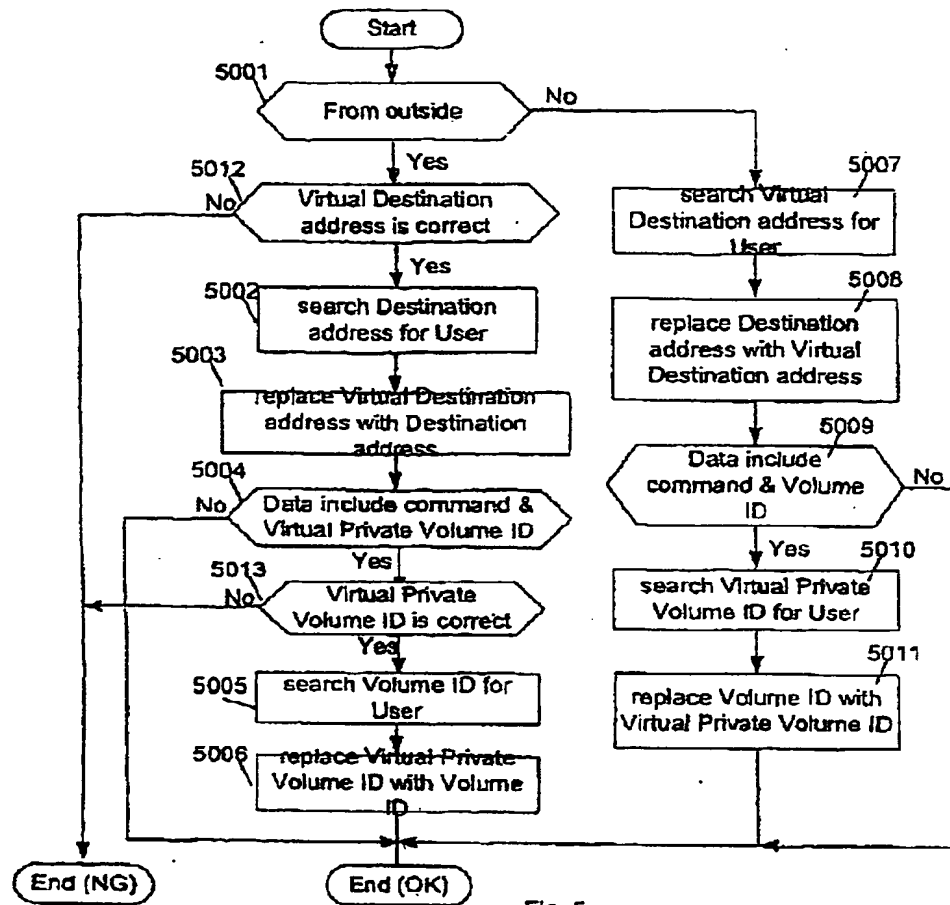


Fig. 5

【図6】

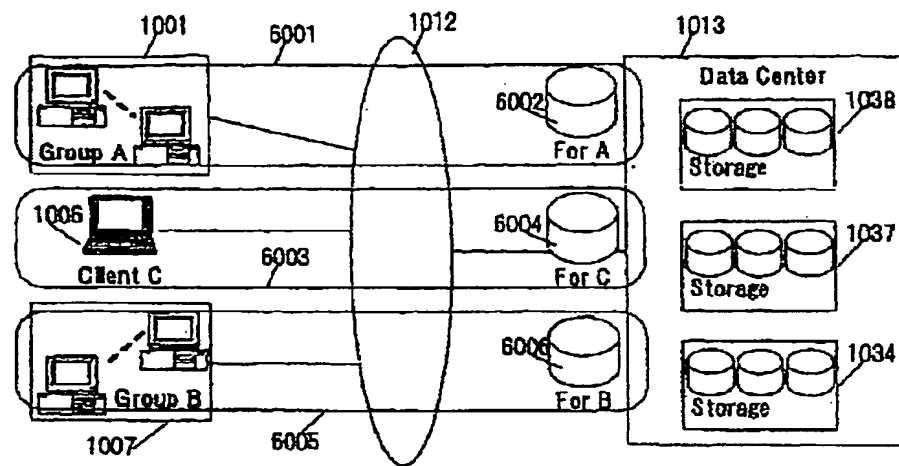


Fig. 6

【図7】

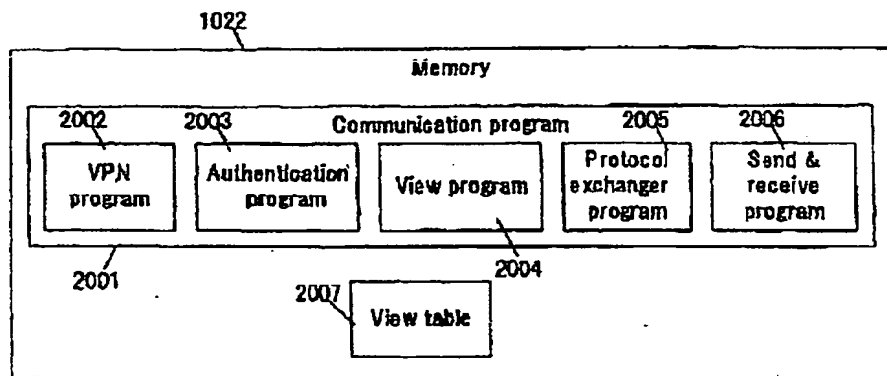


Fig. 7

【 図 8 】

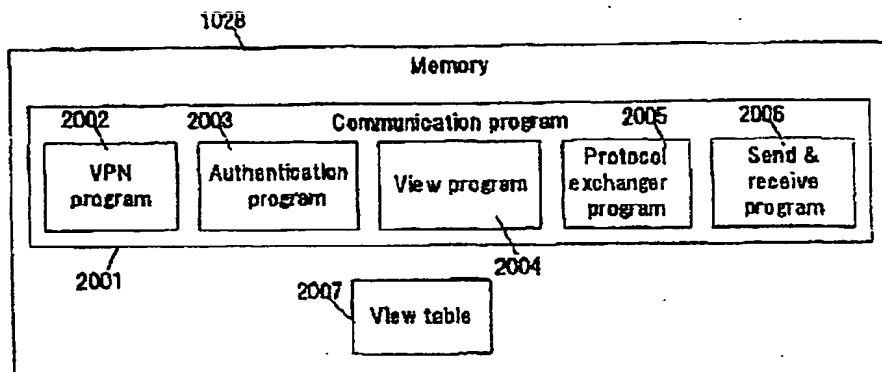


Fig. 8

【 図 9 】

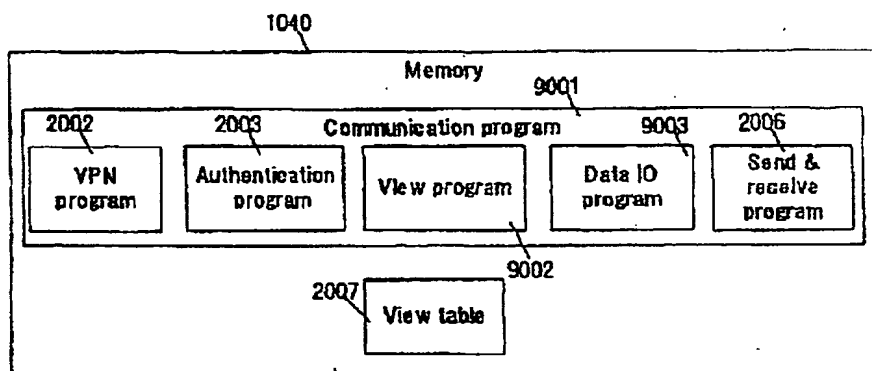


Fig. 9

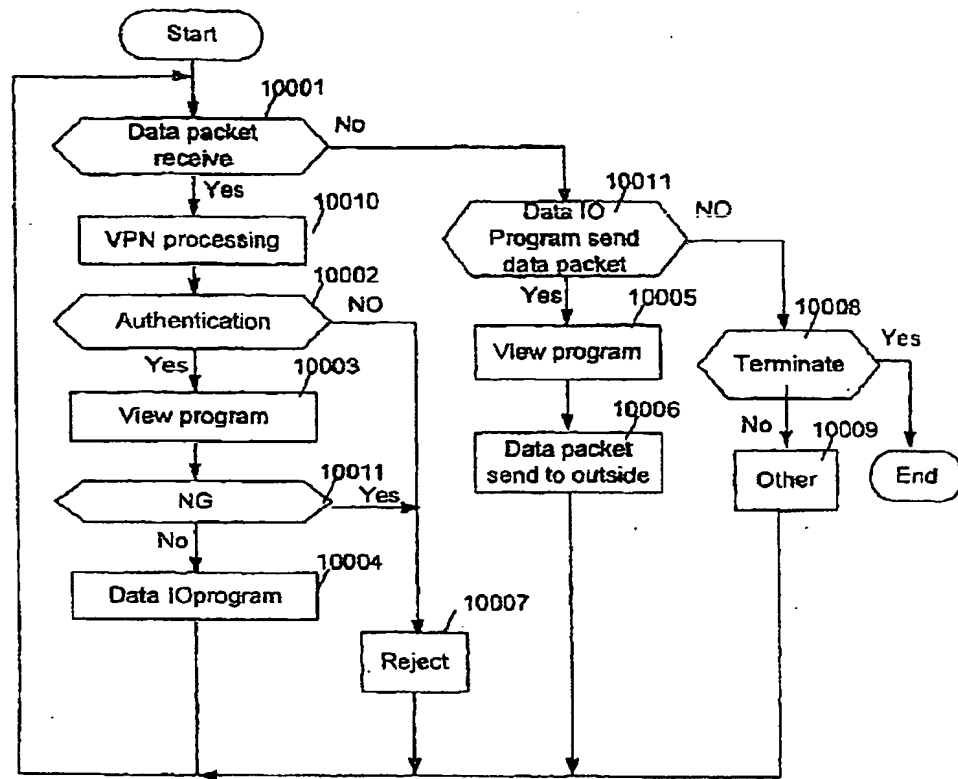


Fig. 10

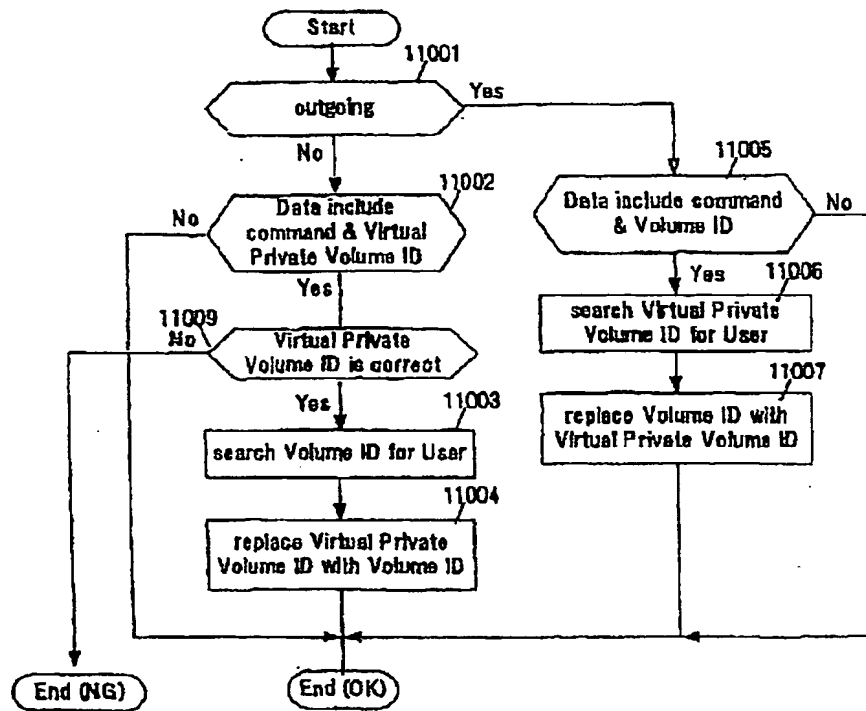


Fig. 11

Virtual Private Volume Method and System

ABSTRACT OF THE DISCLOSURE

5 The present invention provides techniques for managing access to storage
resources. In specific embodiments, storage devices provide storage resources to users
using a system of virtual addresses and virtual volume identifiers. In select specific
embodiments, a storage service provider (SSP) can make volumes available to a user,
which may be a company, for example, in the user's network via the Internet or other
10 kinds of network connections. In specific embodiments, the SSP and the user's data
center can conceal the identity of the storage devices, volumes, and equipment of the
SSP, as well as that of the user's data center in order to provide privacy to both user and
storage provider.

15

20

25

30

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.